SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 April 2021

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-22205	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.	10.0	More Details
CVE-2021-0248	This issue is not applicable to NFX NextGen Software. On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces. This issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX Series devices are affected.	10.0	More Details
CVE-2021-22893	Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been exploited in the wild.	10.0	More Details
CVE-2021-2244	Vulnerability in the Hyperion Analytic Provider Services product of Oracle Hyperion (component: JAPI) and Essbase Analytic Provider Services product of Oracle Essbase (component: JAPI). Supported versions that are affected are Hyperion Analytic Provider Services 11.1.2.4 and 12.2.1.4, and Essbase Analytic Provider Services 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Analytic Provider Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Analytic Provider Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Hyperion Analytic Provider Services. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2248	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop.	10.0	More Details
CVE-2021-2177	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Gateway). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop.	10.0	More Details
CVE-2021-2256	Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Storage Cloud Software Appliance. Note: Updating the Oracle Storage Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download the latest version of Oracle Storage Cloud Software Appliance from <a href=" https://www.oracle.com/downloads/cloud/oscsa-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rstype=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2021-2317	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href=" https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29475	HedgeDoc (formerly known as CodiMD) is an open-source collaborative markdown editor. An attacker is able to receive arbitrary files from the file system when exporting a note to PDF. Since the code injection has to take place as note content, there fore this exploit requires the attackers ability to modify a note. This will affect all instances, which have pdf export enabled. This issue has been fixed by https://github.com/hedgedoc/hedgedoc/commit/c1789474020a6d668d616464cb2da5e90e123f65 and is available in version 1.5.0. Starting the CodiMD/HedgeDoc instance with `CMD_ALLOW_PDF_EXPORT=false` or set `"allowPDFExport": false` in config.json can mitigate this issue for those who cannot upgrade. This exploit works because while PhantomJS doesn't actually render the `file:///` references to the PDF file itself, it still uses them internally, and exfiltration is possible, and easy through JavaScript rendering. The impact is pretty bad, as the attacker is able to read the CodiMD/HedgeDoc `config.json` file as well any other files on the filesystem. Even though the suggested Docker deploy option doesn't have many interesting files itself, the `config.json` still often contains sensitive information, database credentials, and maybe OAuth secrets among other things.	10.0	More Details
CVE-2021-20711	Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors.	9.8	More Details
CVE-2021-25927	Prototype pollution vulnerability in 'safe-flat' versions 2.0.0 through 2.0.1 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-20697	Missing authentication for critical function in DAP-1880AC firmware version 1.21 and earlier allows a remote attacker to login to the device as an authenticated user without the access privilege via unspecified vectors.	9.8	More Details
CVE-2021-31726	Akuvox C315 115.116.2613 allows remote command Injection via the cfgd_server service. The attack vector is sending a payload to port 189 (default root 0.0.0.0).	9.8	More Details
CVE-2021-25928	Prototype pollution vulnerability in 'safe-obj' versions 1.0.0 through 1.0.2 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-26797	An access control vulnerability in Hame SD1 Wi-Fi firmware <=V.20140224154640 allows an attacker to get system administrator through an open Telnet service.	9.8	More Details
CVE-2021-25839	A weak password requirement vulnerability exists in the Create New User function of MintHCM RELEASE 3.0.8, which could lead an attacker to easier password brute-forcing.	9.8	More Details
CVE-2021-30502	The unofficial vscode-ghc-simple (aka Simple Glasgow Haskell Compiler) extension before 0.2.3 for Visual Studio Code allows remote code execution via a crafted workspace configuration with replCommand.	9.8	More Details
CVE-2020-23907	An issue was discovered in retdec v3.3. In function canSplitFunctionOn() of ir_modifications.cpp, there is a possible out of bounds read due to a heap buffer overflow. The impact is: Deny of Service, Memory Disclosure, and Possible Code Execution.	9.8	More Details
CVE-2019-25032	Unbound before 1.9.5 allows an integer overflow in the regional allocator via regional_alloc. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25033	Unbound before 1.9.5 allows an integer overflow in the regional allocator via the ALIGN_UP macro. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details
CVE-2019-25034	Unbound before 1.9.5 allows an integer overflow in sldns_str2wire_dname_buf_origin, leading to an out-of-bounds write. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details
CVE-2019-25035	Unbound before 1.9.5 allows an out-of-bounds write in sldns_bget_token_par. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details
CVE-2019-25038	Unbound before 1.9.5 allows an integer overflow in a size calculation in dnscrypt/dnscrypt.c. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details
CVE-2019-25039	Unbound before 1.9.5 allows an integer overflow in a size calculation in respip/respip.c. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details
CVE-2019-25042	Unbound before 1.9.5 allows an out-of-bounds write via a compressed name in rdata_copy. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	9.8	More Details
CVE-2021-27480	Delta Industrial Automation COMMGR Versions 1.12 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to execute remote code.	9.8	More Details
CVE-2021-30642	An input validation flaw in the Symantec Security Analytics web UI 7.2 prior 7.2.7, 8.1, prior to 8.1.3-NSR3, 8.2, prior to 8.2.1-NSR2 or 8.2.2 allows a remote, unauthenticated attacker to execute arbitrary OS commands on the target with elevated privileges.	9.8	More Details
CVE-2020-22001	HomeAutomation 3.3.2 suffers from an authentication bypass vulnerability when spoofing client IP address using the X-Forwarded-For header with the local (loopback) IP address value allowing remote control of the smart home solution.	9.8	More Details
CVE-2021-29200	Apache OFBiz has unsafe deserialization prior to 17.12.07 version An unauthenticated user can perform an RCE attack	9.8	More Details
CVE-2021-30128	Apache OFBiz has unsafe deserialization prior to 17.12.07 version	9.8	More Details
CVE-2021-31646	Gestsup before 3.2.10 allows account takeover through the password recovery functionality (remote). The affected component is the file forgot_pwd.php - it uses a weak algorithm for the generation of password recovery tokens (the PHP uniqueid function), allowing a brute force attack.	9.8	More Details
CVE-2021-29476	Requests is a HTTP library written in PHP. Requests mishandles deserialization in FilteredIterator. The issue has been patched and users of `Requests` 1.6.0, 1.6.1 and 1.7.0 should update to version 1.8.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2136	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2021-31572	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in stream_buffer.c for a stream buffer.	9.8	More Details
CVE-2021-25668	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.	9.8	More Details
CVE-2021-2135	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Coherence Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2021-21426	Magento-lts is a long-term support alternative to Magento Community Edition (CE). In magento-lts versions 19.4.12 and prior and 20.0.8 and prior, there is a vulnerability caused by the unsecured deserialization of an object. A patch in versions 19.4.13 and 20.0.9 was back ported from Zend Framework 3. The vulnerability was assigned CVE-2021-3007 in Zend Framework.	9.8	More Details
CVE-2021-24240	The Business Hours Pro WordPress plugin through 5.5.0 allows a remote attacker to upload arbitrary files using its manual update functionality, leading to an unauthenticated remote code execution vulnerability.	9.8	More Details
CVE-2021-27389	A vulnerability has been identified in Opcenter Quality (All versions < V12.2), QMS Automotive (All versions < V12.30). A private sign key is shipped with the product without adequate protection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0254	A buffer size validation vulnerability in the overlayd service of Juniper Networks Junos OS may allow an unauthenticated remote attacker to send specially crafted packets to the device, triggering a partial Denial of Service (DoS) condition, or leading to remote code execution (RCE). Continued receipt and processing of these packets will sustain the partial DoS. The overlayd daemon handles Overlay OAM packets, such as ping and traceroute, sent to the overlay. The service runs as root by default and listens for UDP connections on port 4789. This issue results from improper buffer size validation, which can lead to a buffer overflow. Unauthenticated attackers can send specially crafted packets to trigger this vulnerability, resulting in possible remote code execution. overlayd runs by default in MX Series, ACX Series, and QFX Series platforms. The SRX Series does not support VXLAN and is therefore not vulnerable to this issue. Other platforms are also vulnerable if a Virtual Extensible LAN (VXLAN) overlay network is configured. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1.	9.8	More Details
CVE-2021-2302	Vulnerability in the Oracle Platform Security for Java product of Oracle Fusion Middleware (component: OPSS). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Platform Security for Java. Successful attacks of this vulnerability can result in takeover of Oracle Platform Security for Java. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2021-31571	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in queue.c for queue creation.	9.8	More Details
CVE-2021-30476	HashiCorp Terraform's Vault Provider (terraform-provider-vault) did not correctly configure GCE-type bound labels for Vault's GCP auth method. Fixed in 2.19.1.	9.8	More Details
CVE-2021-3287	Zoho ManageEngine OpManager before 12.5.329 allows unauthenticated Remote Code Execution due to a general bypass in the deserialization class.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25669	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.	9.8	More Details
CVE-2021-2221	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop.	9.6	More Details
CVE-2021-21201	Use after free in permissions in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21223	Integer overflow in Mojo in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21226	Use after free in navigation in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-31761	Webmin 1.973 is affected by reflected Cross Site Scripting (XSS) to achieve Remote Command Execution through Webmin's running process feature.	9.6	More Details
CVE-2021-31597	The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected.	9.4	More Details
CVE-2020-17563	Path Traversal in FeiFeiCMS v4.0 allows remote attackers to delete arbitrary files by sending a crafted HTTP request to " /index.php?s=/admin-tpl-del&id=".	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17564	Path Traversal in FeiFeiCMS v4.0 allows remote attackers to delete arbitrary files by sending a crafted HTTP request to the " Admin/DataAction.class.php" component.	9.1	More Details
CVE-2021-2200	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Home page). The supported version that is affected is 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2021-2205	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.7-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2021-2253	Vulnerability in the Oracle Advanced Supply Chain Planning product of Oracle Supply Chain (component: Core). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Supply Chain Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Supply Chain Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Supply Chain Planning accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2021-2318	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href=" https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2319	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href=" https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2021-2320	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href=" https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2021-21427	Magento-lts is a long-term support alternative to Magento Community Edition (CE). A vulnerability in magento-lts versions before 19.4.13 and 20.0.9 potentially allows an administrator unauthorized access to restricted resources. This is a backport of CVE-2021-21024. The vulnerability is patched in versions 19.4.13 and 20.0.9.	9.1	More Details
CVE-2021-26291	Apache Maven will follow repositories that are defined in a dependency's Project Object Model (pom) which may be surprising to some users, resulting in potential risk if a malicious actor takes over that repository or is able to insert themselves into a position to pretend to be that repository. Maven is changing the default behavior in 3.8.1+ to no longer follow http (non-SSL) repository references by default. More details available in the referenced urls. If you are currently using a repository manager to govern the repositories used by your builds, you are unaffected by the risks present in the legacy behavior, and are unaffected by this vulnerability and change to default behavior. See this link for more information about repository management: https://maven.apache.org/repository-management.html	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-29472	Composer is a dependency manager for PHP. URLs for Mercurial repositories in the root composer.json and package source download URLs are not sanitized correctly. Specifically crafted URL values allow code to be executed in the HgDriver if hg/Mercurial is installed on the system. The impact to Composer users directly is limited as the composer.json file is typically under their own control and source download URLs can only be supplied by third party Composer repositories they explicitly trust to download and execute source code from, e.g. Composer plugins. The main impact is to services passing user input to Composer, including Packagist.org and Private Packagist. This allowed users to trigger remote code execution. The vulnerability has been patched on Packagist.org and Private Packagist within 12h of receiving the initial vulnerability report and based on a review of logs, to the best of our knowledge, was not abused by anyone. Other services/tools using VcsRepository/VcsDriver or derivatives may also be vulnerable and should upgrade their composer/composer dependency immediately. Versions 1.10.22 and 2.0.13 include patches for this issue.	8.8	More Details
CVE-2021-20086	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-bbq 1.2.1 allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-20695	Improper following of a certificate's chain of trust vulnerability in DAP-1880AC firmware version 1.21 and earlier allows a remote authenticated attacker to gain root privileges via unspecified vectors.	8.8	More Details
CVE-2021-20694	Improper access control vulnerability in DAP-1880AC firmware version 1.21 and earlier allows a remote authenticated attacker to bypass access restriction and to start a telnet service via unspecified vectors.	8.8	More Details
CVE-2021-31762	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to create a privileged user through Webmin's add users feature, and then get a reverse shell through Webmin's running process feature.	8.8	More Details
CVE-2021-31760	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to achieve Remote Command Execution (RCE) through Webmin's running process feature.	8.8	More Details
CVE-2021-31718	The server in npupnp before 4.1.4 is affected by DNS rebinding in the embedded web server (including UPnP SOAP and GENA endpoints), leading to remote code execution.	8.8	More Details
CVE-2021-31584	Sipwise C5 NGCP www_csc version 3.6.4 up to and including platform NGCP CE mr3.8.13 allows call/click2dial CSRF attacks for actions with administrative privileges.	8.8	More Details
CVE-2021-20089	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in purl 2.3.2 allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-20085	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in backbone-query-parameters 0.4.0 allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-31802	NETGEAR R7000 1.0.11.116 devices have a heap-based Buffer Overflow that is exploitable from the local network without authentication. The vulnerability exists within the handling of an HTTP request. An attacker can leverage this to execute code as root. The problem is that a user-provided length value is trusted during a backup.cgi file upload. The attacker must add a \n before the Content-Length header.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20083	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-plugin-query-object 2.2.3 allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-20088	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in mootools-more 1.6.0 allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-20087	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-deparam 0.5.1 allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-20084	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-sparkle 1.5.2-beta allows a malicious user to inject properties into Object.prototype.	8.8	More Details
CVE-2021-0268	An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') weakness in J-web of Juniper Networks Junos OS leads to buffer overflows, segment faults, or other impacts, which allows an attacker to modify the integrity of the device and exfiltration information from the device without authentication. The weakness can be exploited to facilitate cross-site scripting (XSS), cookie manipulation (modifying session cookies, stealing cookies) and more. This weakness can also be exploited by directing a user to a seemingly legitimate link from the affected site. The attacker requires no special access or permissions to the device to carry out such attacks. This issue affects: Juniper Networks Junos OS: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.1R1.	8.8	More Details
CVE-2021-0269	The improper handling of client-side parameters in J-Web of Juniper Networks Junos OS allows an attacker to perform a number of different malicious actions against a target device when a user is authenticated to J-Web. An attacker may be able to supersede existing parameters, including hardcoded parameters within the HTTP/S session, access and exploit variables, bypass web application firewall rules or input validation mechanisms, and otherwise alter and modify J-Web's normal behavior. An attacker may be able to transition victims to malicious web services, or exfiltrate sensitive information from otherwise secure web forms. This issue affects: Juniper Networks Junos OS: All versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2.	8.8	More Details
CVE-2021-27392	A vulnerability has been identified in Siveillance Video Open Network Bridge (2020 R3), Siveillance Video Open Network Bridge (2020 R2), Siveillance Video Open Network Bridge (2020 R1), Siveillance Video Open Network Bridge (2019 R3), Siveillance Video Open Network Bridge (2019 R2), Siveillance Video Open Network Bridge (2019 R1), Siveillance Video Open Network Bridge (2018 R3), Siveillance Video Open Network Bridge (2018 R2). Affected Open Network Bridges store user credentials for the authentication between ONVIF clients and ONVIF server using a hard-coded key. The encrypted credentials can be retrieved via the MIP SDK. This could allow an authenticated remote attacker to retrieve and decrypt all credentials stored on the ONVIF server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20696	DAP-1880AC firmware version 1.21 and earlier allows a remote authenticated attacker to execute arbitrary OS commands by sending a specially crafted request to a specific CGI program.	8.8	More Details
CVE-2021-0275	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.	8.8	More Details
CVE-2020-21989	HomeAutomation 3.3.2 is affected by Cross Site Request Forgery (CSRF). The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	8.8	More Details
CVE-2021-22669	Incorrect permissions are set to default on the ‘Project Management’ page of WebAccess/SCADA portal of WebAccess/SCADA Versions 9.0.1 and prior, which may allow a low-privileged user to update an administrator’s password and login as an administrator to escalate privileges on the system.	8.8	More Details
CVE-2021-21204	Use after free in Blink in Google Chrome on OS X prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-28269	Soyal Technology 701Client 9.0.1 is vulnerable to Insecure permissions via client.exe binary with Authenticated Users group with Full permissions.	8.8	More Details
CVE-2021-21206	Use after free in Blink in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21203	Use after free in Blink in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21213	Use after free in WebMIDI in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21214	Use after free in Network API in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2021-21220	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21646	Jenkins Templating Engine Plugin 2.1 and earlier does not protect its pipeline configurations using Script Security Plugin, allowing attackers with Job/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM.	8.8	More Details
CVE-2021-28271	Soyal Technologies SOYAL 701Server 9.0.1 suffers from an elevation of privileges vulnerability which can be used by an authenticated user to change the executable file with a binary choice. The vulnerability is due to improper permissions with the 'F' flag (Full) for 'Everyone'and 'Authenticated Users' group.	8.8	More Details
CVE-2021-21224	Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	8.8	More Details
CVE-2021-21225	Out of bounds memory access in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-29441	Nacos is a platform designed for dynamic service discovery and configuration and service management. In Nacos before version 1.4.1, when configured to use authentication (-Dnacos.core.auth.enabled=true) Nacos uses the AuthFilter servlet filter to enforce authentication. This filter has a backdoor that enables Nacos servers to bypass this filter and therefore skip authentication checks. This mechanism relies on the user-agent HTTP header so it can be easily spoofed. This issue may allow any user to carry out any administrative tasks on the Nacos server.	8.6	More Details
CVE-2021-29442	Nacos is a platform designed for dynamic service discovery and configuration and service management. In Nacos before version 1.4.1, the ConfigOpsController lets the user perform management operations like querying the database or even wiping it out. While the /data/remove endpoint is properly protected with the @Secured annotation, the /derby endpoint is not protected and can be openly accessed by unauthenticated users. These endpoints are only valid when using embedded storage (derby DB) so this issue should not affect those installations using external storage (e.g. mysql)	8.6	More Details
CVE-2021-31410	Overly relaxed configuration of frontend resources server in Vaadin Designer versions 4.3.0 through 4.6.3 allows remote attackers to access project sources via crafted HTTP request.	8.6	More Details
CVE-2021-0251	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmand) process thereby denying users the ability to login, while concurrently impacting other mspmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31407	Vulnerability in OSGi integration in com.vaadin:flow-server versions 1.2.0 through 2.4.7 (Vaadin 12.0.0 through 14.4.9), and 6.0.0 through 6.0.1 (Vaadin 19.0.0) allows attacker to access application classes and resources on the server via crafted HTTP request.	8.6	More Details
CVE-2021-21202	Use after free in extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	8.6	More Details
CVE-2021-21207	Use after free in IndexedDB in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	8.6	More Details
CVE-2021-2209	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Email Center. While the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	8.5	More Details
CVE-2020-25244	A vulnerability has been identified in LOGO! Soft Comfort (All versions < V8.4). The software insecurely loads libraries which makes it vulnerable to DLL hijacking. Successful exploitation by a local attacker could lead to a takeover of the system where the software is installed.	8.4	More Details
CVE-2021-2264	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	8.4	More Details
CVE-2020-7861	AnySupport (Remote support solution) before 2019.3.21.0 allows directory traversing because of swprintf function to copy file from a management PC to a client PC. This can be lead to arbitrary file execution.	8.4	More Details
CVE-2021-29465	Discord-Recon is a bot for the Discord chat service. Versions of Discord-Recon 0.0.3 and prior contain a vulnerability in which a remote attacker is able to overwrite any file on the system with the command results. This can result in remote code execution when the user overwrite important files on the system. As a workaround, bot maintainers can edit their `setting.py` file then add `<` and `>` into the `RCE` variable inside of it to fix the issue without an update. The vulnerability is patched in version 0.0.4.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2218	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Health Center). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L).	8.3	More Details
CVE-2021-2198	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-20454	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196649.	8.2	More Details
CVE-2021-2250	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2021-2242	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27278	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.1-49141. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the current user on the host system. Was ZDI-CAN-12130.	8.2	More Details
CVE-2021-2210	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2206	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2199	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2186	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2197	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2150	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2188	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2187	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2185	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2184	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2183	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2182	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-2195	Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Attribute Admin Setup). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-20501	IBM i 7.1, 7.2, 7.3, and 7.4 SMTP allows a network attacker to send emails to non-existent local-domain recipients to the SMTP server, caused by using a non-default configuration. An attacker could exploit this vulnerability to consume unnecessary network bandwidth and disk space, and allow remote attackers to send spam email. IBM X-Force ID: 198056.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2236	Vulnerability in the Oracle Financials Common Modules product of Oracle E-Business Suite (component: Advanced Global Intercompany). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials Common Modules. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financials Common Modules accessible data as well as unauthorized access to critical data or complete access to all Oracle Financials Common Modules accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-27009	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), Nucleus NET (All versions < V5.2), Nucleus Source Code (Versions including affected DNS modules), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.	8.1	More Details
CVE-2021-2235	Vulnerability in the Oracle Transportation Execution product of Oracle E-Business Suite (component: Install and Upgrade). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Execution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Execution accessible data as well as unauthorized access to critical data or complete access to all Oracle Transportation Execution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2233	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Setup). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Asset Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2231	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Installed Base accessible data as well as unauthorized access to critical data or complete access to all Oracle Installed Base accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2225	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Intelligence accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2228	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2227	Vulnerability in the Oracle Cash Management product of Oracle E-Business Suite (component: Bank Account Transfer). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cash Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Cash Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Cash Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2156	Vulnerability in the Oracle Customers Online product of Oracle E-Business Suite (component: Customer Tab). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Customers Online. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Customers Online accessible data as well as unauthorized access to critical data or complete access to all Oracle Customers Online accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2224	Vulnerability in the Oracle Compensation Workbench product of Oracle E-Business Suite (component: Compensation Workbench). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Compensation Workbench. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Compensation Workbench accessible data as well as unauthorized access to critical data or complete access to all Oracle Compensation Workbench accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2223	Vulnerability in the Oracle Receivables product of Oracle E-Business Suite (component: Receipts). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Receivables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Receivables accessible data as well as unauthorized access to critical data or complete access to all Oracle Receivables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2222	Vulnerability in the Oracle Bill Presentment Architecture product of Oracle E-Business Suite (component: Template Search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bill Presentment Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Bill Presentment Architecture accessible data as well as unauthorized access to critical data or complete access to all Oracle Bill Presentment Architecture accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2238	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Process Operations). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle MES for Process Manufacturing accessible data as well as unauthorized access to critical data or complete access to all Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2237	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Account Hierarchy Manager). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2255	Vulnerability in the Oracle Service Contracts product of Oracle E-Business Suite (component: Authoring). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Service Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Service Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2239	Vulnerability in the Oracle Time and Labor product of Oracle E-Business Suite (component: Timecard). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Time and Labor. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Time and Labor accessible data as well as unauthorized access to critical data or complete access to all Oracle Time and Labor accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2241	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iStore accessible data as well as unauthorized access to critical data or complete access to all Oracle iStore accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2273	Vulnerability in the Oracle Legal Entity Configurator product of Oracle E-Business Suite (component: Create Contracts). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Legal Entity Configurator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Legal Entity Configurator accessible data as well as unauthorized access to critical data or complete access to all Oracle Legal Entity Configurator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2274	Vulnerability in the Oracle E-Business Tax product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Business Tax. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Tax accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Tax accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2276	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSetup accessible data as well as unauthorized access to critical data or complete access to all Oracle iSetup accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2279	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2021-2288	Vulnerability in the Oracle Bills of Material product of Oracle E-Business Suite (component: Bill Issues). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bills of Material. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Bills of Material accessible data as well as unauthorized access to critical data or complete access to all Oracle Bills of Material accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2289	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Template, GTIN search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2290	Vulnerability in the Oracle Engineering product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Engineering. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Engineering accessible data as well as unauthorized access to critical data or complete access to all Oracle Engineering accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2292	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Document Management). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Document Management and Collaboration accessible data as well as unauthorized access to critical data or complete access to all Oracle Document Management and Collaboration accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2295	Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite (component: BI Publisher Integration). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Concurrent Processing accessible data as well as unauthorized access to critical data or complete access to all Oracle Concurrent Processing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2314	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Profiles). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Application Object Library accessible data as well as unauthorized access to critical data or complete access to all Oracle Application Object Library accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2316	Vulnerability in the Oracle HRMS (France) product of Oracle E-Business Suite (component: French HR). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle HRMS (France). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HRMS (France) accessible data as well as unauthorized access to critical data or complete access to all Oracle HRMS (France) accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-7385	By launching the drb_remote_codeexec exploit, a Metasploit Framework user will inadvertently expose Metasploit to the same deserialization issue that is exploited by that module, due to the reliance on the vulnerable Distributed Ruby class functions. Since Metasploit Framework typically runs with elevated privileges, this can lead to a system compromise on the Metasploit workstation. Note that an attacker would have to lie in wait and entice the Metasploit user to run the affected module against a malicious endpoint in a "hack-back" type of attack. Metasploit is only vulnerable when the drb_remote_codeexec module is running. In most cases, this cannot happen automatically.	8.1	More Details
CVE-2020-7035	An XML External Entities (XXE)vulnerability in the web-based user interface of Avaya Aura Orchestration Designer could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Orchestration Designer includes all 7.x versions before 7.2.3.	8.1	More Details
CVE-2020-7036	An XML External Entities (XXE)vulnerability in Callback Assist could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Callback Assist includes all 4.0.x versions before 4.7.1.1 Patch 7.	8.1	More Details
CVE-2021-21205	Insufficient policy enforcement in navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	8.1	More Details
CVE-2021-2272	Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Inquiries). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Subledger Accounting accessible data as well as unauthorized access to critical data or complete access to all Oracle Subledger Accounting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2271	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Resource Exceptions). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2270	Vulnerability in the Oracle Site Hub product of Oracle E-Business Suite (component: Sites). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Site Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Site Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Site Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2258	Vulnerability in the Oracle Projects product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Projects. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Projects accessible data as well as unauthorized access to critical data or complete access to all Oracle Projects accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2246	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2247	Vulnerability in the Oracle Advanced Collections product of Oracle E-Business Suite (component: Admin). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Collections. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Collections accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Collections accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2249	Vulnerability in the Oracle Landed Cost Management product of Oracle E-Business Suite (component: Shipment Workbench). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Landed Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Landed Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Landed Cost Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2251	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Data Source). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Technical Foundation accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2252	Vulnerability in the Oracle Loans product of Oracle E-Business Suite (component: Loan Details, Loan Accounting Events). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Loans. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Loans accessible data as well as unauthorized access to critical data or complete access to all Oracle Loans accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2254	Vulnerability in the Oracle Project Contracts product of Oracle E-Business Suite (component: Hold Management). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Project Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Project Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2259	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: India Localization, Results). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payables accessible data as well as unauthorized access to critical data or complete access to all Oracle Payables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2269	Vulnerability in the Oracle Advanced Pricing product of Oracle E-Business Suite (component: Price Book). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Pricing accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Pricing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2260	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: iRecruitment). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2261	Vulnerability in the Oracle Lease and Finance Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Lease and Finance Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Lease and Finance Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Lease and Finance Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2262	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Endeca). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Purchasing accessible data as well as unauthorized access to critical data or complete access to all Oracle Purchasing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2263	Vulnerability in the Oracle Sourcing product of Oracle E-Business Suite (component: Intelligence, RFx). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sourcing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sourcing accessible data as well as unauthorized access to critical data or complete access to all Oracle Sourcing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2267	Vulnerability in the Oracle Labor Distribution product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Labor Distribution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Labor Distribution accessible data as well as unauthorized access to critical data or complete access to all Oracle Labor Distribution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-15795	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), Nucleus NET (All versions < V5.2), Nucleus Source Code (Versions including affected DNS modules), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). The DNS domain name label parsing functionality does not properly validate the names in DNS-responses. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2268	Vulnerability in the Oracle Quoting product of Oracle E-Business Suite (component: Courseware). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quoting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Quoting accessible data as well as unauthorized access to critical data or complete access to all Oracle Quoting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2229	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: LOVs). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Depot Repair accessible data as well as unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-30356	A denial of service vulnerability was reported in Check Point Identity Agent before R81.018.0000, which could allow low privileged users to overwrite protected system files.	8.1	More Details
CVE-2021-0249	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT:	8.1	More Details
CVE-2021-0266	The use of multiple hard-coded cryptographic keys in cSRX Series software in Juniper Networks Junos OS allows an attacker to take control of any instance of a cSRX deployment through device management services. This issue affects: Juniper Networks Junos OS on cSRX Series: All versions prior to 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2.	8.1	More Details
CVE-2021-21642	Jenkins Config File Provider Plugin 3.7.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.1	More Details
CVE-2021-0265	An unvalidated REST API in the AppFormix Agent of Juniper Networks AppFormix allows an unauthenticated remote attacker to execute commands as root on the host running the AppFormix Agent, when certain preconditions are performed by the attacker, thus granting the attacker full control over the environment. This issue affects: Juniper Networks AppFormix 3 versions prior to 3.1.22, 3.2.14, 3.3.0.	8.1	More Details
CVE-2020-22000	HomeAutomation 3.3.2 suffers from an authenticated OS command execution vulnerability using custom command v0.1 plugin. This can be exploited with a CSRF vulnerability to execute arbitrary shell commands as the web user via the 'set_command_on' and 'set_command_off' POST parameters in '/system/systemplugins/customcommand/customcommand.plugin.php' by using an unsanitized PHP exec() function.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35979	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is heap-based buffer overflow in the function gp_rtp_builder_do_avc() in ietf/rtp_pck_mpeg4.c.	7.8	More Details
CVE-2020-35980	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is a use-after-free in the function gf_isom_box_del() in isomedia/box_funcs.c.	7.8	More Details
CVE-2021-22678	Cscape (All versions prior to 9.90 SP4) lacks proper validation of user-supplied data when parsing project files. This could lead to memory corruption. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-20532	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 could allow a local user to escalate their privileges to take full control of the system due to insecure directory permissions. IBM X-Force ID: 198811.	7.8	More Details
CVE-2021-29667	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.2 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 199403.	7.8	More Details
CVE-2021-31607	In SaltStack Salt 2016.9 through 3002.6, a command injection vulnerability exists in the snapper module that allows for local privilege escalation on a minion. The attack requires that a file is created with a pathname that is backed up by snapper, and that the master calls the snapper.diff function (which executes popen unsafely).	7.8	More Details
CVE-2021-3464	A DLL search path vulnerability was reported in Lenovo PCManager, prior to version 3.0.400.3252, that could allow privilege escalation.	7.8	More Details
CVE-2021-2167	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2021-22660	CNCSoft-B Versions 1.0.0.3 and prior is vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-29672	IBM Spectrum Protect Client 8.1.0.0-8 through 1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing the current locale settings. A local attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges or cause the application to crash. IBM X-Force ID: 199479	7.8	More Details
CVE-2021-31784	An out-of-bounds write vulnerability exists in the file-reading procedure in Open Design Alliance Drawings SDK before 2021.6 on all supported by ODA platforms in static configuration. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart) or possible code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0245	A Use of Hard-coded Credentials vulnerability in Juniper Networks Junos OS on Junos Fusion satellite devices allows an attacker who is local to the device to elevate their privileges and take control of the device. This issue affects: Juniper Networks Junos OS Junos Fusion Satellite Devices. 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3-S2; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10; 17.4 version 17.4R3 and later versions; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2; 20.1 versions prior to 20.1R1-S1, 20.1R2. This issue does not affected Junos OS releases prior to 16.1R1 or all 19.2R3 and 19.4R3 release versions.	7.8	More Details
CVE-2021-27277	This vulnerability allows local attackers to escalate privileges on affected installations of SolarWinds Orion Virtual Infrastructure Monitor 2020.2. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the OneTimeJobSchedulerEventsService WCF service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-11955.	7.8	More Details
CVE-2021-22682	Cscape (All versions prior to 9.90 SP4) is configured by default to be installed for all users, which allows full permissions, including read/write access. This may allow unprivileged users to modify the binaries and configuration files and lead to local privilege escalation.	7.8	More Details
CVE-2021-3496	A heap-based buffer overflow was found in jhead in version 3.06 in Get16u() in exif.c when processing a crafted file.	7.8	More Details
CVE-2020-35982	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is an invalid pointer dereference in the function gf_hinter_track_finalize() in media_tools/isom_hinter.c.	7.8	More Details
CVE-2021-0253	NFX Series devices using Juniper Networks Junos OS are susceptible to a local command execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series 17.2 version 17.2R1 and later versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S3; 19.2 version 19.1R2 and later versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S2. 19.4 versions 19.4R3 and above. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.	7.8	More Details
CVE-2021-0252	NFX Series devices using Juniper Networks Junos OS are susceptible to a local code execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series: 18.1 version 18.1R1 and later versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 18.1R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22664	CNCSoft-B Versions 1.0.0.3 and prior is vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2020-35981	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is an invalid pointer dereference in the function SetupWriters() in isomedia/isom_store.c.	7.8	More Details
CVE-2021-31523	The Debian xscreensaver 5.42+dfsg1-1 package for XScreenSaver has cap_net_raw enabled for the /usr/libexec/xscreensaver/sonar file, which allows local users to gain privileges because this is arguably incompatible with the design of the Mesa 3D Graphics library dependency.	7.8	More Details
CVE-2020-26997	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (All versions < SE2020MP14), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11919)	7.8	More Details
CVE-2021-3472	A flaw was found in xorg-x11-server in versions before 1.20.11. An integer underflow can occur in xserver which can lead to a local privilege escalation. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2021-25678	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (All versions < SE2020MP14), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12529)	7.8	More Details
CVE-2021-28648	Trend Micro Antivirus for Mac 2020 v10.5 and 2021 v11 (Consumer) is vulnerable to an improper access control privilege escalation vulnerability that could allow an attacker to establish a connection that could lead to full local privilege escalation within the application. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	7.8	More Details
CVE-2021-25670	A vulnerability has been identified in Tecnomatix RobotExpert (All versions < V16.1). Affected applications lack proper validation of user-supplied data when parsing CELL files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12608)	7.8	More Details
CVE-2021-27382	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (All versions < SE2020MP14), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13040)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29460	Kirby is an open source CMS. An editor with write access to the Kirby Panel can upload an SVG file that contains harmful content like `<script>` tags. The direct link to that file can be sent to other users or visitors of the site. If the victim opens that link in a browser where they are logged in to Kirby, the script will run and can for example trigger requests to Kirby's API with the permissions of the victim. This vulnerability is critical if you might have potential attackers in your group of authenticated Panel users, as they can escalate their privileges if they get access to the Panel session of an admin user. Depending on your site, other JavaScript-powered attacks are possible. Visitors without Panel access can only use this attack vector if your site allows SVG file uploads in frontend forms and you don't already sanitize uploaded SVG files. The problem has been patched in Kirby 3.5.4. Please update to this or a later version to fix the vulnerability. Frontend upload forms need to be patched separately depending on how they store the uploaded file(s). If you use `File::create()`, you are protected by updating to 3.5.4+. As a work around you can disable the upload of SVG files in your file blueprints.	7.6	More Details
CVE-2021-2181	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Attachments). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. While the vulnerability is in Oracle Document Management and Collaboration, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Document Management and Collaboration accessible data as well as unauthorized update, insert or delete access to some of Oracle Document Management and Collaboration accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N).	7.6	More Details
CVE-2021-2277	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2019-25036	Unbound before 1.9.5 allows an assertion failure and denial of service in synth_cname. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	7.5	More Details
CVE-2019-25037	Unbound before 1.9.5 allows an assertion failure and denial of service in dname_pkt_copy via an invalid packet. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	7.5	More Details
CVE-2019-25040	Unbound before 1.9.5 allows an infinite loop via a compressed name in dname_pkt_copy. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	7.5	More Details
CVE-2021-2190	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29653	HashiCorp Vault and Vault Enterprise 1.5.1 and newer, under certain circumstances, may exclude revoked but unexpired certificates from the CRL. Fixed in 1.5.8, 1.6.4, and 1.7.1.	7.5	More Details
CVE-2021-27400	HashiCorp Vault and Vault Enterprise Cassandra integrations (storage backend and database secrets engine plugin) did not validate TLS certificates when connecting to Cassandra clusters. Fixed in 1.6.4 and 1.7.1	7.5	More Details
CVE-2021-31598	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode() performs incorrect memory handling while parsing crafted XML files, leading to a heap-based buffer overflow.	7.5	More Details
CVE-2021-2189	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-0261	A vulnerability in the HTTP/HTTPS service used by J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Captive Portal allows an unauthenticated attacker to cause an extended Denial of Service (DoS) for these services by sending a high number of specific requests. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S17 on EX Series; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 15.1 versions prior to 15.1R7-S8; 15.1X49 versions prior to 15.1X49-D230 on SRX Series; 16.1 versions prior to 16.1R7-S8; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2.	7.5	More Details
CVE-2021-31555	An issue was discovered in the Oauth extension for MediaWiki through 1.35.2. It did not validate the oarc_version (aka oauth_registered_consumer.oarc_version) parameter's length.	7.5	More Details
CVE-2020-27568	Insecure File Permissions exist in Aviatrix Controller 5.3.1516. Several world writable files and directories were found in the controller resource. Note: All Aviatrix appliances are fully encrypted. This is an extra layer of security.	7.5	More Details
CVE-2021-25899	An issue was discovered in svc-login.php in Void Aural Rec Monitor 9.0.0.1. An unauthenticated attacker can send a crafted HTTP request to perform a blind time-based SQL Injection. The vulnerable parameter is param1.	7.5	More Details
CVE-2021-31791	In Hardware Sentry KM before 10.0.01 for BMC PATROL, a cleartext password may be discovered after a failure or timeout of a command.	7.5	More Details
CVE-2021-20693	Improper access control vulnerability in Gurunavi App for Android ver.10.0.10 and earlier and for iOS ver.11.1.2 and earlier allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20590	Improper authentication vulnerability in GOT2000 series GT27 model VNC server versions 01.39.010 and prior, GOT2000 series GT25 model VNC server versions 01.39.010 and prior, GOT2000 series GT21 model GT2107-WTBD VNC server versions 01.40.000 and prior, GOT2000 series GT21 model GT2107-WTSD VNC server versions 01.40.000 and prior, GOT SIMPLE series GS21 model GS2110-WTBD-N VNC server versions 01.40.000 and prior and GOT SIMPLE series GS21 model GS2107-WTBD-N VNC server versions 01.40.000 and prior allows a remote unauthenticated attacker to gain unauthorized access via specially crafted packets when the "VNC server" function is used.	7.5	More Details
CVE-2020-28973	The ABUS Secvest wireless alarm system FUAA50000 (v3.01.17) fails to properly authenticate some requests to its built-in HTTPS interface. Someone can use this vulnerability to obtain sensitive information from the system, such as usernames and passwords. This information can then be used to reconfigure or disable the alarm system.	7.5	More Details
CVE-2021-31826	Shibboleth Service Provider 3.x before 3.2.2 is prone to a NULL pointer dereference flaw involving the session recovery feature. The flaw is exploitable (for a daemon crash) on systems not using this feature if a crafted cookie is supplied.	7.5	More Details
CVE-2021-0227	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;	7.5	More Details
CVE-2021-0230	On Juniper Networks SRX Series devices with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding | match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding | match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue affects Juniper Networks Junos OS on SRX Series: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.	7.5	More Details
CVE-2021-31671	pgsync before 0.6.7 is affected by Information Disclosure of sensitive information. Syncing the schema with the --schema-first and --schema-only options is mishandled. For example, the sslmode connection parameter may be lost, which means that SSL would not be used.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0233	A vulnerability in Juniper Networks Junos OS ACX500 Series, ACX4000 Series, may allow an attacker to cause a Denial of Service (DoS) by sending a high rate of specific packets to the device, resulting in a Forwarding Engine Board (FFEB) crash. Continued receipt of these packets will sustain the Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on ACX500 Series, ACX4000 Series: 17.4 versions prior to 17.4R3-S2.	7.5	More Details
CVE-2021-30165	The default administrator account & password of the EDIMAX wireless network camera is hard-coded. Remote attackers can disassemble firmware to obtain the privileged permission and further control the devices.	7.5	More Details
CVE-2021-31783	show_default.php in the LocalFilesEditor extension before 11.4.0.1 for Piwigo allows Local File Inclusion because the file parameter is not validated with a proper regular-expression check.	7.5	More Details
CVE-2020-36325	An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, there's an out-of-bounds read-access bug. NOTE: the vendor reports that this only occurs when a programmer fails to follow the API specification	7.5	More Details
CVE-2021-0250	In segment routing traffic engineering (SRTE) environments where the BGP Monitoring Protocol (BMP) feature is enable, a vulnerability in the Routing Protocol Daemon (RPD) process of Juniper Networks Junos OS allows an attacker to send a specific crafted BGP update message causing the RPD service to core, creating a Denial of Service (DoS) Condition. Continued receipt and processing of this update message will create a sustained Denial of Service (DoS) condition. This issue affects IPv4 and IPv6 environments. This issue affects: Juniper Networks Junos OS 17.4 versions 17.4R1 and above prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2, This issue does not affect Junos OS releases prior to 17.4R1. This issue affects: Juniper Networks Junos OS Evolved 19.2-EVO versions prior to 19.2R2-EVO.	7.5	More Details
CVE-2021-29694	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 200258.	7.5	More Details
CVE-2020-15078	OpenVPN 2.5.1 and earlier versions allows a remote attackers to bypass authentication and access control channel data on servers configured with deferred authentication, which can be used to potentially trigger further information leaks.	7.5	More Details
CVE-2021-25663	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (All versions including affected IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values.	7.5	More Details
CVE-2021-28965	The REXML gem before 3.2.5 in Ruby before 2.6.7, 2.7.x before 2.7.3, and 3.x before 3.0.1 does not properly address XML round-trip issues. An incorrect document can be produced after parsing and serializing.	7.5	More Details
CVE-2019-25041	Unbound before 1.9.5 allows an assertion failure via a compressed name in dname_pkt_copy. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25898	An issue was discovered in svc-login.php in Void Aural Rec Monitor 9.0.0.1. Passwords are stored in unencrypted source-code text files. This was noted when accessing the svc-login.php file. The value is used to authenticate a high-privileged user upon authenticating with the server.	7.5	More Details
CVE-2021-30638	Information Exposure vulnerability in context asset handling of Apache Tapestry allows an attacker to download files inside WEB-INF if using a specially-constructed URL. This was caused by an incomplete fix for CVE-2020-13953. This issue affects Apache Tapestry Apache Tapestry 5.4.0 version to Apache Tapestry 5.6.3; Apache Tapestry 5.7.0 version and Apache Tapestry 5.7.1.	7.5	More Details
CVE-2021-31405	Unsafe validation RegEx in EmailField component in com.vaadin:vaadin-text-field-flow versions 2.0.4 through 2.3.2 (Vaadin 14.0.6 through 14.4.3), and 3.0.0 through 4.0.2 (Vaadin 15.0.0 through 17.0.10) allows attackers to cause uncontrolled resource consumption by submitting malicious email addresses.	7.5	More Details
CVE-2021-2157	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: TopLink Integration). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2021-2145	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2020-36320	Unsafe validation RegEx in EmailValidator class in com.vaadin:vaadin-server versions 7.0.0 through 7.7.21 (Vaadin 7.0.0 through 7.7.21) allows attackers to cause uncontrolled resource consumption by submitting malicious email addresses.	7.5	More Details
CVE-2021-2310	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2021-2309	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30139	In Alpine Linux apk-tools before 2.12.5, the tarball parser allows a buffer overflow and crash.	7.5	More Details
CVE-2021-0270	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.	7.5	More Details
CVE-2021-31780	In app/Model/MispObject.php in MISP 2.4.141, an incorrect sharing group association could lead to information disclosure on an event edit. When an object has a sharing group associated with an event edit, the sharing group object is ignored and instead the passed local ID is reused.	7.5	More Details
CVE-2021-25664	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (All versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values.	7.5	More Details
CVE-2020-17517	The S3 buckets and keys in a secure Apache Ozone Cluster must be inaccessible to anonymous access by default. The current security vulnerability allows access to keys and buckets through a curl command or an unauthenticated HTTP request. This enables unauthorized access to buckets and keys thereby exposing data to anonymous clients or users. This affected Apache Ozone prior to the 1.1.0 release.	7.5	More Details
CVE-2020-27569	Arbitrary File Write exists in Aviatrix VPN Client 2.8.2 and earlier. The VPN service writes logs to a location that is world writable and can be leveraged to gain write access to any file on the system.	7.5	More Details
CVE-2021-0241	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash with a core dump if a specific DHCPv6 packet is received, resulting in a restart of the daemon. The daemon automatically restarts without intervention, but continued receipt and processing of these specific packets will repeatedly crash the JDHCPD process and sustain the Denial of Service (DoS) condition. This issue only affects DHCPv6. DHCPv4 is not affected by this issue. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1, 19.3R3-S2; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2219	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L).	7.4	More Details
CVE-2021-0244	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages	grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.	7.4	More Details
CVE-2021-0267	An Improper Input Validation vulnerability in the active-lease query portion in JDHCPD's DHCP Relay Agent of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending a crafted DHCP packet to the device thereby crashing the jdhcpd DHCP service. This is typically configured for Broadband Subscriber Sessions. Continued receipt and processing of this crafted packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS Evolved.	7.4	More Details
CVE-2021-0240	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, the Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash if a malformed DHCPv6 packet is received, resulting in a restart of the daemon. The daemon automatically restarts without intervention, but continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects DHCPv6. DHCPv4 is not affected by this issue. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0232	An authentication bypass vulnerability in the Juniper Networks Paragon Active Assurance Control Center may allow an attacker with specific information about the deployment to mimic an already registered Test Agent and access its configuration including associated inventory details. If the issue occurs, the affected Test Agent will not be able to connect to the Control Center. This issue affects Juniper Networks Paragon Active Assurance Control Center All versions prior to 2.35.6; 2.36 versions prior to 2.36.2.	7.4	More Details
CVE-2021-0259	Due to a vulnerability in DDoS protection in Juniper Networks Junos OS and Junos OS Evolved on QFX5K Series switches in a VXLAN configuration, instability might be experienced in the underlay network as a consequence of exceeding the default ddos-protection aggregate threshold. If an attacker on a client device on the overlay network sends a high volume of specific, legitimate traffic in the overlay network, due to an improperly detected DDoS violation, the leaf might not process certain L2 traffic, sent by spines in the underlay network. Continued receipt and processing of the high volume traffic will sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX5K Series: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S2, 20.3R2. Juniper Networks Junos OS Evolved on QFX5220: All versions prior to 20.3R2-EVO.	7.4	More Details
CVE-2021-0235	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0246	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.	7.3	More Details
CVE-2021-1075	NVIDIA Windows GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the program dereferences a pointer that contains a location for memory that is no longer valid, which may lead to code execution, denial of service, or escalation of privileges. Attacker does not have any control over the information and may conduct limited data modification.	7.3	More Details
CVE-2021-1074	NVIDIA GPU Display Driver for Windows installer contains a vulnerability where an attacker with local unprivileged system access may be able to replace an application resource with malicious files. This attack requires a user with system administration rights to execute the installer and requires the attacker to replace the files in a very short time window between file integrity validation and execution. Such an attack may lead to code execution, escalation of privileges, denial of service, and information disclosure.	7.3	More Details
CVE-2021-2240	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details
CVE-2021-2008	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected are 11.1.1.9 and 12.2.1.3 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager for Fusion Middleware accessible data as well as unauthorized read access to a subset of Enterprise Manager for Fusion Middleware accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0260	An improper authorization vulnerability in the Simple Network Management Protocol daemon (snmpd) service of Juniper Networks Junos OS leads an unauthenticated attacker being able to perform SNMP read actions, an Exposure of System Data to an Unauthorized Control Sphere, or write actions to OIDs that support write operations, against the device without authentication. This issue affects: Juniper Networks Junos OS: 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S6, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.	7.3	More Details
CVE-2020-7034	A command injection vulnerability in Avaya Session Border Controller for Enterprise could allow an authenticated, remote attacker to send specially crafted messages and execute arbitrary commands with the affected system privileges. Affected versions of Avaya Session Border Controller for Enterprise include 7.x, 8.0 through 8.1.1.x	7.2	More Details
CVE-2021-2144	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2021-20709	Improper validation of integrity check value vulnerability in NEC Aterm WF1200CR firmware Ver1.3.2 and earlier, Aterm WG1200CR firmware Ver1.3.3 and earlier, and Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to a specific URL.	7.2	More Details
CVE-2021-20708	NEC Aterm devices (Aterm WF1200CR firmware Ver1.3.2 and earlier, Aterm WG1200CR firmware Ver1.3.3 and earlier, and Aterm WG2600HS firmware Ver1.5.1 and earlier) allow authenticated attackers to execute arbitrary OS commands by sending a specially crafted request to a specific URL.	7.2	More Details
CVE-2021-2280	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	7.1	More Details
CVE-2021-2282	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2283	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	7.1	More Details
CVE-2021-2284	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	7.1	More Details
CVE-2021-2285	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	7.1	More Details
CVE-2020-23922	An issue was discovered in giflib through 5.1.4. DumpScreen2RGB in gif2rgb.c has a heap-based buffer over-read.	7.1	More Details
CVE-2021-2286	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	7.1	More Details
CVE-2021-2287	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	7.1	More Details
CVE-2020-23921	An issue was discovered in fast_ber through v0.4. yy::yylex() in asn_compiler.hpp has a heap-based buffer over-read.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2281	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	7.1	More Details
CVE-2020-23931	An issue was discovered in gpac before 1.0.1. The abst_box_read function in box_code_adobe.c has a heap-based buffer over-read.	7.1	More Details
CVE-2020-23928	An issue was discovered in gpac before 1.0.1. The abst_box_read function in box_code_adobe.c has a heap-based buffer over-read.	7.1	More Details
CVE-2021-31540	Wowza Streaming Engine through 4.8.5 (in a default installation) has incorrect file permissions of configuration files in the conf/ directory. A regular local user is able to read and write to all the configuration files, e.g., modify the application server configuration.	7.1	More Details
CVE-2021-0226	On Juniper Networks Junos OS Evolved devices, receipt of a specific IPv6 packet may cause an established IPv6 BGP session to terminate, creating a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue does not affect IPv4 BGP sessions. This issue affects IBGP or EBGP peer sessions with IPv6. This issue affects: Juniper Networks Junos OS Evolved: 19.4 versions prior to 19.4R2-S3-EVO; 20.1 versions prior to 20.1R2-S3-EVO; 20.2 versions prior to 20.2R2-S1-EVO; 20.3 versions prior to 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS releases.	7.1	More Details
CVE-2021-31795	The PowerVR GPU kernel driver in pvrsrvkm.ko through 2021-04-24 for the Linux kernel, as used on Alcatel 1S phones, allows attackers to overwrite heap memory via PhysmemNewRamBackedPMR.	7.0	More Details
CVE-2020-7858	There is a directory traversing vulnerability in the download page url of AquaNPlayer 2.0.0.92. The IP of the download page url is localhost and an attacker can traverse directories using "dot dot" sequences(../../) to view host file on the system. This vulnerability can cause information leakage.	6.8	More Details
CVE-2021-22204	Improper neutralization of user data in the DjVu file format in ExifTool versions 7.44 and up allows arbitrary code execution when parsing the malicious image	6.8	More Details
CVE-2021-23133	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation from the context of a network service or an unprivileged process. If sctp_destroy_sock is called without sock_net(sk)->sctp.addr_wq_lock then an element is removed from the auto_asconf_splist list without any proper locking. This can be exploited by an attacker with network service privileges to escalate to root or from the context of an unprivileged user directly if a BPF_CGROUP_INET_SOCK_CREATE is attached which denies creation of some SCTP socket.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2151	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).	6.7	More Details
CVE-2021-1077	NVIDIA GPU Display Driver for Windows and Linux, R450 and R460 driver branch, contains a vulnerability where the software uses a reference count to manage a resource that is incorrectly updated, which may lead to denial of service.	6.6	More Details
CVE-2021-1076	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys or nvidia.ko) where improper access control may lead to denial of service, information disclosure, or data corruption.	6.6	More Details
CVE-2021-21222	Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2021-21216	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details
CVE-2021-21212	Incorrect security UI in Network Config UI in Google Chrome on ChromeOS prior to 90.0.4430.72 allowed a remote attacker to potentially compromise WiFi connection security via a malicious WAP.	6.5	More Details
CVE-2021-21215	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details
CVE-2021-31548	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. A MediaWiki user who is partially blocked or was unsuccessfully blocked could bypass AbuseFilter and have their edits completed.	6.5	More Details
CVE-2021-2298	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2021-21210	Inappropriate implementation in Network in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially access local UDP ports via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2294	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	6.5	More Details
CVE-2021-2172	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2021-2178	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2021-20714	Directory traversal vulnerability in WP Fastest Cache versions prior to 0.9.1.7 allows a remote attacker with administrator privileges to delete arbitrary files on the server via unspecified vectors.	6.5	More Details
CVE-2021-31553	An issue was discovered in the CheckUser extension for MediaWiki through 1.35.2. MediaWiki usernames with trailing whitespace could be stored in the cu_log database table such that denial of service occurred for certain CheckUser extension pages and functionality. For example, the attacker could turn off Special:CheckUserLog and thus interfere with usage tracking.	6.5	More Details
CVE-2021-21211	Inappropriate implementation in Navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0242	A vulnerability due to the improper handling of direct memory access (DMA) buffers on EX4300 switches on Juniper Networks Junos OS allows an attacker sending specific unicast frames to trigger a Denial of Service (DoS) condition by exhausting DMA buffers, causing the FPC to crash and the device to restart. The DMA buffer leak is seen when receiving these specific, valid unicast frames on an interface without Layer 2 Protocol Tunneling (L2PT) or dot1x configured. Interfaces with either L2PT or dot1x configured are not vulnerable to this issue. When this issue occurs, DMA buffer usage keeps increasing and the following error log messages may be observed: Apr 14 14:29:34.360 /kernel: pid 64476 (pfex_junos), uid 0: exited on signal 11 (core dumped) Apr 14 14:29:33.790 init: pfe-manager (PID 64476) terminated by signal number 11. Core dumped! The DMA buffers on the FPC can be monitored by the executing vty command 'show heap': ID Base Total(b) Free(b) Used(b) % Name -- ---------- ---------- ---------- ---------- --- ---------- 0 4a46000 268435456 238230496 30204960 11 Kernel 1 18a46000 67108864 17618536 49490328 73 Bcm_sdk 2 23737000 117440512 18414552 99025960 84 DMA buf <<<<< keeps increasing 3 2a737000 16777216 16777216 0 0 DMA desc This issue affects Juniper Networks Junos OS on the EX4300: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2.	6.5	More Details
CVE-2021-2311	Vulnerability in the Oracle Hospitality Inventory Management product of Oracle Food and Beverage Applications (component: Export to Reporting and Analytics). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Inventory Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Inventory Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2021-21209	Inappropriate implementation in storage in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-0262	Through routine static code analysis of the Juniper Networks Junos OS software codebase, the Secure Development Life Cycle team identified a Use After Free vulnerability in PFE packet processing on the QFX10002-60C switching platform. Exploitation of this vulnerability may allow a logically adjacent attacker to trigger a Denial of Service (DoS). Continued exploitation of this vulnerability will sustain the Denial of Service (DoS) condition. This issue only affects QFX10002-60C devices. No other product or platform is vulnerable to this issue. This issue affects Juniper Networks Junos OS on QFX10002-60C: 19.1 version 19.1R3-S1 and later versions; 19.1 versions prior to 19.1R3-S3; 19.2 version 19.2R2 and later versions; 19.2 versions prior to 19.2R3-S1; 20.2 versions prior to 20.2R1-S2. This issue does not affect Juniper Networks Junos OS: versions prior to 19.1R3; 19.2 versions prior to 19.2R2; any version of 19.3; version 20.2R2 and later releases.	6.5	More Details
CVE-2021-29466	Discord-Recon is a bot for the Discord chat service. In versions of Discord-Recon 0.0.3 and prior, a remote attacker is able to read local files from the server that can disclose important information. As a workaround, a bot maintainer can locate the file `app.py` and add `.replace('..', '')` into the `Path` variable inside of the `recon` function. The vulnerability is patched in version 0.0.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2134	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected is 12.2.1.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2021-20432	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 196344.	6.5	More Details
CVE-2021-21643	Jenkins Config File Provider Plugin 3.7.0 and earlier does not correctly perform permission checks in several HTTP endpoints, allowing attackers with global Job/Configure permission to enumerate system-scoped credentials IDs of credentials stored in Jenkins.	6.5	More Details
CVE-2021-0271	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.	6.5	More Details
CVE-2021-24238	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not ensure that the requested property to be deleted belong to the user making the request, allowing any authenticated users to delete arbitrary properties by tampering with the property_id parameter.	6.5	More Details
CVE-2021-28167	In Eclipse Openj9 to version 0.25.0, usage of the jdk.internal.reflect.ConstantPool API causes the JVM in some cases to pre-resolve certain constant pool entries. This allows a user to call static methods or access static members without running the class initialization method, and may allow a user to observe uninitialized values.	6.5	More Details
CVE-2020-27738	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.3), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (Versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a read access past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27737	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.3), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (Versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). The DNS response parsing functionality does not properly validate various length and counts of the records. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the memory past the allocated structure.	6.5	More Details
CVE-2020-27736	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.3), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (Versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). The DNS domain name label parsing functionality does not properly validate the null-terminated name in DNS-responses. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the read memory.	6.5	More Details
CVE-2021-0272	A kernel memory leak in QFX10002-32Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016 devices Flexible PIC Concentrators (FPCs) on Juniper Networks Junos OS allows an attacker to send genuine packets destined to the device to cause a Denial of Service (DoS) to the device. On QFX10002-32Q, QFX10002-60C, QFX10002-72Q devices the device will crash and restart. On QFX10008, QFX10016 devices, depending on the number of FPCs involved in an attack, one more more FPCs may crash and traffic through the device may be degraded in other ways, until the attack traffic stops. A reboot is required to restore service and clear the kernel memory. Continued receipt and processing of these genuine packets will create a sustained Denial of Service (DoS) condition. On QFX10008, QFX10016 devices, an indicator of compromise may be the existence of DCPFE core files. You can also monitor PFE memory utilization for incremental growth: user@qfx-RE:0% cprod -A fpc0 -c "show heap 0"	grep -i ke 0 3788a1b0 3221225048 2417120656 804104392 24 Kernel user@qfx-RE:0% cprod -A fpc0 -c "show heap 0"	grep -i ke 0 3788a1b0 3221225048 2332332200 888892848 27 Kernel This issue affects: Juniper Networks Junos OS on QFX10002-32Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016: 16.1 versions 16.1R1 and above prior to 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2. This issue does not affect releases prior to Junos OS 16.1R1. This issue does not affect EX Series devices. This issue does not affect Junos OS Evolved.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2275	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2021-21208	Insufficient data validation in QR scanner in Google Chrome on iOS prior to 90.0.4430.72 allowed an attacker displaying a QR code to perform domain spoofing via a crafted QR code.	6.5	More Details
CVE-2021-27736	FusionAuth fusionauth-samlv2 before 0.5.4 allows XXE attacks via a forged AuthnRequest or LogoutRequest because parseFromBytes uses javax.xml.parsers.DocumentBuilderFactory unsafely.	6.5	More Details
CVE-2021-0237	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2;	6.5	More Details
CVE-2021-0228	An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN-(Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief | match lacp This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;	6.5	More Details
CVE-2021-0231	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2202	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2021-21221	Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-0224	A vulnerability in the handling of internal resources necessary to bring up a large number of Layer 2 broadband remote access subscriber (BRAS) nodes in Juniper Networks Junos OS can cause the Access Node Control Protocol daemon (ANCPD) to crash and restart, leading to a Denial of Service (DoS) condition. Continued processing of spoofed subscriber nodes will create a sustained Denial of Service (DoS) condition. When the number of subscribers attempting to connect exceeds the configured maximum-discovery-table-entries value, the subscriber fails to map to an internal neighbor entry, causing the ANCPD process to crash. This issue affects Juniper Networks Junos OS: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R2.	6.5	More Details
CVE-2021-0216	A vulnerability in Juniper Networks Junos OS running on the ACX5448 and ACX710 platforms may cause BFD sessions to flap when a high rate of transit ARP packets are received. This, in turn, may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. When a high rate of transit ARP packets are exceptioned to the CPU and BFD flaps, the following log messages may be seen: bfdd[15864]: BFDD_STATE_UP_TO_DOWN: BFD Session 192.168.14.3 (IFL 232) state Up -> Down LD/RD(17/19) Up time:11:38:17 Local diag: CtlExpire Remote diag: None Reason: Detect Timer Expiry. bfdd[15864]: BFDD_TRAP_SHOP_STATE_DOWN: local discriminator: 17, new state: down, interface: irb.998, peer addr: 192.168.14.3 rpd[15839]: RPD_ISIS_ADJDOWN: IS-IS lost L2 adjacency to peer on irb.998, reason: BFD Session Down bfdd[15864]: BFDD_TRAP_SHOP_STATE_UP: local discriminator: 17, new state: up, interface: irb.998, peer addr: 192.168.14.3 This issue only affects the ACX5448 Series and ACX710 Series routers. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 18.2 versions prior to 18.2R3-S8 on ACX5448; 18.3 versions prior to 18.3R3-S5 on ACX5448; 18.4 versions prior to 18.4R1-S6, 18.4R3-S7 on ACX5448; 19.1 versions prior to 19.1R3-S5 on ACX5448; 19.2 versions prior to 19.2R2, 19.2R3 on ACX5448; 19.3 versions prior to 19.3R3 on ACX5448; 19.4 versions prior to 19.4R3 on ACX5448; 20.1 versions prior to 20.1R2 on ACX5448; 20.2 versions prior to 20.2R2 on ACX5448 and ACX710.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0214	A vulnerability in the distributed or centralized periodic packet management daemon (PPMD) of Juniper Networks Junos OS may cause receipt of a malformed packet to crash and restart the PPMD process, leading to network destabilization, service interruption, and a Denial of Service (DoS) condition. Continued receipt and processing of these malformed packets will repeatedly crash the PPMD process and sustain the Denial of Service (DoS) condition. Due to the nature of the specifically crafted packet, exploitation of this issue requires direct, adjacent connectivity to the vulnerable component. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S12, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S5, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.	6.5	More Details
CVE-2021-0236	Due to an improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved the Routing Protocol Daemon (RPD) service, upon receipt of a specific matching BGP packet meeting a specific term in the flowspec configuration, crashes and restarts causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects only Multiprotocol BGP (MP-BGP) VPNv6 FlowSpec deployments. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS Evolved: All versions after 18.4R1-EVO prior to 20.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved versions prior to 18.4R1-EVO.	6.5	More Details
CVE-2021-0257	On Juniper Networks MX Series and EX9200 Series platforms with Trio-based MPCs (Modular Port Concentrators) where Integrated Routing and Bridging (IRB) interfaces are configured and mapped to a VPLS instance or a Bridge-Domain, certain Layer 2 network events at Customer Edge (CE) devices may cause memory leaks in the MPC of Provider Edge (PE) devices which can cause an out of memory condition and MPC restart. When this issue occurs, there will be temporary traffic interruption until the MPC is restored. An administrator can use the following CLI command to monitor the status of memory usage level of the MPC: user@device> show system resource-monitor fpc FPC Resource Usage Summary Free Heap Mem Watermark : 20 % Free NH Mem Watermark : 20 % Free Filter Mem Watermark : 20 % * - Watermark reached Slot # % Heap Free RTT Average RTT 1 87 PFE # % ENCAP mem Free % NH mem Free % FW mem Free 0 NA 88 99 1 NA 89 99 When the issue is occurring, the value of “% NH mem Free” will go down until the MPC restarts. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines), including MX-MPC1-3D, MX-MPC1E-3D, MX-MPC2-3D, MX-MPC2E-3D, MPC-3D-16XGE, and CHAS-MXxx Series MPCs. No other products or platforms are affected by this issue. This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S3; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.2 versions prior to 20.2R1-S3, 20.2R2; 20.3 versions prior to 20.3R1-S1,, 20.3R2. This issue does not affect Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R3-S2; 18.1; 18.2 versions prior to 18.2R3-S4; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R3-S1; 19.1; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0239	In Juniper Networks Junos OS Evolved, receipt of a stream of specific genuine Layer 2 frames may cause the Advanced Forwarding Toolkit (AFT) manager process (Evo-aftmand), responsible for handling Route, Class-of-Service (CoS), Firewall operations within the packet forwarding engine (PFE) to crash and restart, leading to a Denial of Service (DoS) condition. By continuously sending this specific stream of genuine Layer 2 frames, an attacker can repeatedly crash the PFE, causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R1-EVO. This issue does not affect Junos OS versions.	6.5	More Details
CVE-2021-31408	Authentication.logout() helper in com.vaadin:flow-client versions 5.0.0 prior to 6.0.0 (Vaadin 18), and 6.0.0 through 6.0.4 (Vaadin 19.0.0 through 19.0.3) uses incorrect HTTP method, which, in combination with Spring Security CSRF protection, allows local attackers to access Fusion endpoints after the user attempted to log out.	6.3	More Details
CVE-2021-20536	IBM Spectrum Protect Plus File Systems Agent 10.1.6 and 10.1.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 198836.	6.2	More Details
CVE-2021-28168	Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local information disclosure vulnerability. This is due to the use of the File.createTempFile which creates a file inside of the system temporary directory with the permissions: -rw-r--r--. Thus the contents of this file are viewable by all other users locally on the system. As such, if the contents written is security sensitive, it can be disclosed to other local users.	6.2	More Details
CVE-2021-28079	Jamovi <=1.6.18 is affected by a cross-site scripting (XSS) vulnerability. The column-name is vulnerable to XSS in the ElectronJS Framework. An attacker can make a .omv (Jamovi) document containing a payload. When opened by victim, the payload is triggered.	6.1	More Details
CVE-2021-2053	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: UI Framework). The supported version that is affected is 13.4.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Enterprise Manager Base Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2021-22540	Bad validation logic in the Dart SDK versions prior to 2.12.3 allow an attacker to use an XSS attack via DOM clobbering. The validation logic in dart:html for creating DOM nodes from text did not sanitize properly when it came across template tags.	6.1	More Details
CVE-2021-2140	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Rules Framework). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2142	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2021-25838	The Import function in MintHCM RELEASE 3.0.8 allows an attacker to execute a cross-site scripting (XSS) payload in file-upload.	6.1	More Details
CVE-2021-2307	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	6.1	More Details
CVE-2020-21998	In HomeAutomation 3.3.2 input passed via the 'redirect' GET parameter in 'api.php' script is not properly verified before being used to redirect users. This can be exploited to redirect a user to an arbitrary website e.g. when a user clicks a specially crafted link to the affected script hosted on a trusted domain.	6.1	More Details
CVE-2021-25382	An improper authorization of using debugging command in Secure Folder prior to SMR Oct-2020 Release 1 allows unauthorized access to contents in Secure Folder via debugging command.	6.1	More Details
CVE-2021-29467	Wrongthink is an encrypted peer-to-peer chat program. A user could check their fingerprint into the service and enter a script to run arbitrary JavaScript on the site. No workarounds exist, but a patch exists in version 2.4.1.	6.1	More Details
CVE-2019-25027	Missing output sanitization in default RouteNotFoundError view in com.vaadin:flow-server versions 1.0.0 through 1.0.10 (Vaadin 10.0.0 through 10.0.13), and 1.1.0 through 1.4.2 (Vaadin 11.0.0 through 13.0.5) allows attacker to execute malicious JavaScript via crafted URL	6.1	More Details
CVE-2020-21987	HomeAutomation 3.3.2 is affected by persistent Cross Site Scripting (XSS). XSS vulnerabilities occur when input passed via several parameters to several scripts is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session.	6.1	More Details
CVE-2021-31803	cPanel before 94.0.3 allows self-XSS via EasyApache 4 Save Profile (SEC-581).	6.1	More Details
CVE-2021-24233	The Cooked Pro WordPress plugin before 1.7.5.6 was affected by unauthenticated reflected Cross-Site Scripting issues, due to improper sanitisation of user input while being output back in pages as an arbitrary attribute.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31794	Settings.aspx?view=About in Directum 5.8.2 allows XSS via the HTTP User-Agent header.	6.1	More Details
CVE-2021-2216	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Multichannel Framework). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2021-24234	The Search Forms page of the Ivory Search WordPress lugin before 4.6.1 did not properly sanitise the tab parameter before output it in the page, leading to a reflected Cross-Site Scripting issue when opening a malicious crafted link as a high privilege user. Knowledge of a form id is required to conduct the attack.	6.1	More Details
CVE-2021-31551	An issue was discovered in the PageForms extension for MediaWiki through 1.35.2. Crafted payloads for Token-related query parameters allowed for XSS on certain PageForms-managed MediaWiki pages.	6.1	More Details
CVE-2021-24235	The Goto WordPress theme before 2.0 does not sanitise the keywords and start_date GET parameter on its Tour List page, leading to an unauthenticated reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2021-20680	Cross-site scripting vulnerability in NEC Aterm devices (Aterm WG1900HP2 firmware Ver.1.3.1 and earlier, Aterm WG1900HP firmware Ver.2.5.1 and earlier, Aterm WG1800HP4 firmware Ver.1.3.1 and earlier, Aterm WG1800HP3 firmware Ver.1.5.1 and earlier, Aterm WG1200HS2 firmware Ver.2.5.0 and earlier, Aterm WG1200HP3 firmware Ver.1.3.1 and earlier, Aterm WG1200HP2 firmware Ver.2.5.0 and earlier, Aterm W1200EX firmware Ver.1.3.1 and earlier, Aterm W1200EX-MS firmware Ver.1.3.1 and earlier, Aterm WG1200HS firmware all versions Aterm WG1200HP firmware all versions Aterm WF800HP firmware all versions Aterm WF300HP2 firmware all versions Aterm WR8165N firmware all versions Aterm W500P firmware all versions, and Aterm W300P firmware all versions) allows remote attackers to inject arbitrary script or HTML via unspecified vectors.	6.1	More Details
CVE-2021-20710	Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.5.1 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-24237	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not properly sanitise the keyword_search, search_radius. _bedrooms and _bathrooms GET parameters before outputting them in its properties page, leading to an unauthenticated reflected Cross-Site Scripting issue.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2192	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris as well as unauthorized update, insert or delete access to some of Oracle Solaris accessible data. Note: This vulnerability applies to Oracle Solaris on SPARC systems only. CVSS 3.1 Base Score 6.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	6.1	More Details
CVE-2021-24239	The Pie Register – User Registration Forms. Invitation based registrations, Custom Login, Payments WordPress plugin before 3.7.0.1 does not sanitise the invitaion_code GET parameter when outputting it in the Activation Code page, leading to a reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2021-24241	The Advanced Custom Fields Pro WordPress plugin before 5.9.1 did not properly escape the generated update URL when outputting it in an attribute, leading to a reflected Cross-Site Scripting issue in the update settings page.	6.1	More Details
CVE-2020-36324	Wikimedia Quarry analytics-quarry-web before 2020-12-15 allows Reflected XSS because app.py does not explicitly set the application/json content type.	6.1	More Details
CVE-2021-28125	Apache Superset up to and including 1.0.1 allowed for the creation of an external URL that could be malicious. By not checking user input for open redirects the URL shortener functionality would allow for a malicious user to create a short URL for a dashboard that could convince the user to click the link.	6.1	More Details
CVE-2021-2306	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2021-2266	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-4981	IBM Spectrum Scale 5.0.4.1 through 5.1.0.3 could allow a local privileged user to overwrite files due to improper input validation. IBM X-Force ID: 192541.	6.0	More Details
CVE-2020-36321	Improper URL validation in development mode handler in com.vaadin:flow-server versions 2.0.0 through 2.4.1 (Vaadin 14.0.0 through 14.4.2), and 3.0 prior to 5.0 (Vaadin 15 prior to 18) allows attacker to request arbitrary files stored outside of intended frontend resources folder.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2211	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details
CVE-2021-3494	A smart proxy that provides a restful API to various sub-systems of the Foreman is affected by the flaw which can cause a Man-in-the-Middle attack. The FreeIPA module of Foreman smart proxy does not check the SSL certificate, thus, an unauthenticated attacker can perform actions in FreeIPA if certain conditions are met. The highest threat from this flaw is to system confidentiality. This flaw affects Foreman versions before 2.5.0.	5.9	More Details
CVE-2019-25031	Unbound before 1.9.5 allows configuration injection in create_unbound_ad_servers.sh upon a successful man-in-the-middle attack against a cleartext HTTP session. NOTE: The vendor does not consider this a vulnerability of the Unbound software. create_unbound_ad_servers.sh is a contributed script from the community that facilitates automatic configuration creation. It is not part of the Unbound installation	5.9	More Details
CVE-2021-0263	A Data Processing vulnerability in the Multi-Service process (multi-svcs) on the FPC of Juniper Networks Junos OS on the PTX Series routers may lead to the process becoming unresponsive, ultimately affecting traffic forwarding, allowing an attacker to cause a Denial of Service (DoS) condition . The Multi-Service Process running on the FPC is responsible for handling sampling-related operations when a J-Flow configuration is activated. This can occur during periods of heavy route churn, causing the Multi-Service Process to stop processing updates, without consuming any further updates from kernel. This back pressure towards the kernel affects further dynamic updates from other processes in the system, including RPD, causing a KRT-STUCK condition and traffic forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. The following logs/alarms will be observed when this condition exists: user@junos> show chassis alarms 2 alarms currently active Alarm time Class Description 2020-10-11 04:33:45 PDT Minor Potential slow peers are: MSP(FPC1-PIC0) MSP(FPC3-PIC0) MSP(FPC4-PIC0) Logs: Oct 11 04:33:44.672 2020 test /kernel: rts_peer_cp_recv_timeout : Bit set for msp8 as it is stuck Oct 11 04:35:56.000 2020 test-lab fpc4 user.err gldfpc-multi-svcs.elf: Error in parsing composite nexthop Oct 11 04:35:56.000 2020 test-lab fpc4 user.err gldfpc-multi-svcs.elf: composite nexthop parsing error Oct 11 04:43:05 2020 test /kernel: rt_pfe_veto: Possible slowest client is msp38. States processed - 65865741. States to be processed - 0 Oct 11 04:55:55 2020 test /kernel: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (8311787520) Current delayed unref = (60000), Current unique delayed unref = (10896), Max delayed unref on this platform = (40000) Current delayed weight unref = (71426) Max delayed weight unref on this platform= (400000) curproc = rpd Oct 11 04:56:00 2020 test /kernel: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 This issue only affects PTX Series devices. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS on PTX Series: 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.2R1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0264	A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	5.9	More Details
CVE-2021-2161	Vulnerability in the Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u291, 8u281, 11.0.10, 16; Java SE Embedded: 8u281; Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2 and 21.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. It can also be exploited by supplying untrusted data to APIs in the specified Component. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	5.9	More Details
CVE-2021-0258	A vulnerability in the forwarding of transit TCPv6 packets received on the Ethernet management interface of Juniper Networks Junos OS allows an attacker to trigger a kernel panic, leading to a Denial of Service (DoS). Continued receipt and processing of these transit packets will create a sustained Denial of Service (DoS) condition. This issue only occurs when TCPv6 packets are routed through the management interface. Other transit traffic, and traffic destined to the management interface, are unaffected by this vulnerability. This issue was introduced as part of a TCP Parallelization feature added in Junos OS 17.2, and affects systems with concurrent network stack enabled. This feature is enabled by default, but can be disabled (see WORKAROUND section below). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0234	Due to an improper Initialization vulnerability on Juniper Networks Junos OS QFX5100-96S devices with QFX 5e Series image installed, ddos-protection configuration changes will not take effect beyond the default DDoS (Distributed Denial of Service) settings when configured from the CLI. The DDoS protection (jddosd) daemon allows the device to continue to function while protecting the packet forwarding engine (PFE) during the DDoS attack. When this issue occurs, the default DDoS settings within the PFE apply, as CPU bound packets will be throttled and dropped in the PFE when the limits are exceeded. To check if the device has this issue, the administrator can execute the following command to monitor the status of DDoS protection: user@device> show ddos-protection protocols error: the ddos-protection subsystem is not running This issue affects only QFX5100-96S devices. No other products or platforms are affected by this issue. This issue affects: Juniper Networks Junos OS on QFX5100-96S: 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R3, 19.1R3-S4; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2;	5.8	More Details
CVE-2021-0225	An Improper Check for Unusual or Exceptional Conditions in Juniper Networks Junos OS Evolved may cause the stateless firewall filter configuration which uses the action 'policer' in certain combinations with other options to not take effect. An administrator can use the following CLI command to see the failures with filter configuration: user@device> show log kfirewall-agent.log | match ERROR Jul 23 14:16:03 ERROR: filter not supported This issue affects Juniper Networks Junos OS Evolved: Versions 19.1R1-EVO and above prior to 20.3R1-S2-EVO, 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS.	5.8	More Details
CVE-2021-29456	Authelia is an open-source authentication and authorization server providing 2-factor authentication and single sign-on (SSO) for your applications via a web portal. In versions 4.27.4 and earlier, utilizing a HTTP query parameter an attacker is able to redirect users from the web application to any domain, including potentially malicious sites. This security issue does not directly impact the security of the web application itself. As a workaround, one can use a reverse proxy to strip the query parameter from the affected endpoint. There is a patch for version 4.28.0.	5.7	More Details
CVE-2021-22207	Excessive memory consumption in MS-WSP dissector in Wireshark 3.4.0 to 3.4.4 and 3.2.0 to 3.2.12 allows denial of service via packet injection or crafted capture file	5.5	More Details
CVE-2021-0255	A local privilege escalation vulnerability in ethtraceroute of Juniper Networks Junos OS may allow a locally authenticated user with shell access to escalate privileges and write to the local filesystem as root. ethtraceroute is shipped with setuid permissions enabled and is owned by the root user, allowing local users to run ethtraceroute with root privileges. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D240; 17.3 versions prior to 17.3R3-S11, 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1.	5.5	More Details
CVE-2021-21217	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	5.5	More Details
CVE-2020-23932	An issue was discovered in gpac before 1.0.1. A NULL pointer dereference exists in the function dump_isom_sdp located in filedump.c. It allows an attacker to cause Denial of Service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21218	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	5.5	More Details
CVE-2021-2304	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2020-23930	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function nhmldump_send_header located in write_nhml.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-3451	A denial of service vulnerability was reported in Lenovo PCManager, prior to version 3.0.400.3252, that could allow configuration files to be written to non-standard locations.	5.5	More Details
CVE-2021-0256	A sensitive information disclosure vulnerability in the mosquitto message broker of Juniper Networks Junos OS may allow a locally authenticated user with shell access the ability to read portions of sensitive files, such as the master.passwd file. Since mosquitto is shipped with setuid permissions enabled and is owned by the root user, this vulnerability may allow a local privileged user the ability to run mosquitto with root privileges and access sensitive information stored on the local filesystem. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S12, 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.3 versions prior to 18.3R3-S4; 19.1 versions prior to 19.1R3-S4; 19.3 versions prior to 19.3R3-S1, 19.3R3-S2; 19.4 versions prior to 19.4R2-S3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2, 20.2R3.	5.5	More Details
CVE-2020-23912	An issue was discovered in Bento4 through v1.6.0-637. A NULL pointer dereference exists in the function AP4_StszAtom::GetSampleSize() located in Ap4StszAtom.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2020-23914	An issue was discovered in cpp-peglib through v0.1.12. A NULL pointer dereference exists in the peg::AstOptimizer::optimize() located in peglib.h. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-1078	NVIDIA Windows GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel driver (nvlddmkm.sys) where a NULL pointer dereference may lead to system crash.	5.5	More Details
CVE-2021-31804	LeoCAD before 21.03 sometimes allows a use-after-free during the opening of a new document.	5.5	More Details
CVE-2021-31539	Wowza Streaming Engine before 4.8.8.01 (in a default installation) has cleartext passwords stored in the conf/admin.password file. A regular local user is able to read usernames and passwords.	5.5	More Details
CVE-2020-23915	An issue was discovered in cpp-peglib through v0.1.12. peg::resolve_escape_sequence() in peglib.h has a heap-based buffer over-read.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27851	A security vulnerability that can lead to local privilege escalation has been found in 'guix-daemon'. It affects multi-user setups in which 'guix-daemon' runs locally. The attack consists in having an unprivileged user spawn a build process, for instance with `guix build`, that makes its build directory world-writable. The user then creates a hardlink to a root-owned file such as /etc/shadow in that build directory. If the user passed the --keep-failed option and the build eventually fails, the daemon changes ownership of the whole build tree, including the hardlink, to the user. At that point, the user has write access to the target file. Versions after and including v0.11.0-3298-g2608e40988, and versions prior to v1.2.0-75109-g94f0312546 are vulnerable.	5.5	More Details
CVE-2021-20546	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and cause the application to crash. IBM X-Force ID: 198934	5.5	More Details
CVE-2021-0238	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.	5.5	More Details
CVE-2021-21219	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	5.5	More Details
CVE-2021-2220	Vulnerability in the PeopleSoft Enterprise SCM eProcurement product of Oracle PeopleSoft (component: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2021-31712	react-draft-wysiwyg (aka React Draft Wysiwyg) before 1.14.6 allows a javascript: URi in a Link Target of the link decorator in decorators/Link/index.js when a draft is shared across users, leading to XSS.	5.4	More Details
CVE-2020-35542	Unisys Data Exchange Management Studio through 5.0.34 doesn't sanitize the input to a HTML document field. This could be used for an XSS attack.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2191	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2021-31550	An issue was discovered in the CommentBox extension for MediaWiki through 1.35.2. Via crafted configuration variables, a malicious actor could introduce XSS payloads into various layers.	5.4	More Details
CVE-2021-31552	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly executed certain rules related to blocking accounts after account creation. Such rules would allow for user accounts to be created while blocking only the IP address used to create an account (and not the user account itself). Such rules could also be used by a nefarious, unprivileged user to catalog and enumerate any number of IP addresses related to these account creations.	5.4	More Details
CVE-2021-24232	The Advanced Booking Calendar WordPress plugin before 1.6.8 does not sanitise the license error message when output in the settings page, leading to an authenticated reflected Cross-Site Scripting issue	5.4	More Details
CVE-2021-20550	IBM Content Navigator 3.0.CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199168.	5.4	More Details
CVE-2021-21644	A cross-site request forgery (CSRF) vulnerability in Jenkins Config File Provider Plugin 3.7.0 and earlier allows attackers to delete configuration files corresponding to an attacker-specified ID.	5.4	More Details
CVE-2021-31583	Sipwise C5 NGCP WWW Admin version 3.6.7 up to and including platform version NGCP CE 3.0 has multiple authenticated stored and reflected XSS vulnerabilities when input passed via several parameters to several scripts is not properly sanitized before being returned to the user: Stored XSS in callforward/time/set/save (POST tsetname); Reflected XSS in addressbook (GET filter); Stored XSS in addressbook/save (POST firstname, lastname, company); and Reflected XSS in statistics/versions (GET lang).	5.4	More Details
CVE-2021-20448	IBM Content Navigator 3.0.CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196624.	5.4	More Details
CVE-2021-29666	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199400.	5.4	More Details
CVE-2019-25028	Missing variable sanitization in Grid component in com.vaadin:vaadin-server versions 7.4.0 through 7.7.19 (Vaadin 7.4.0 through 7.7.19), and 8.0.0 through 8.8.4 (Vaadin 8.0.0 through 8.8.4) allows attacker to inject malicious JavaScript via unspecified vector	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31554	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It improperly handled account blocks for certain automatically created MediaWiki user accounts, thus allowing nefarious users to remain unblocked.	5.4	More Details
CVE-2021-31329	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Chat" and "Personal Address" field on staff/register.php	5.4	More Details
CVE-2021-20549	IBM Content Navigator 3.0.CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199167.	5.4	More Details
CVE-2021-31327	Stored XSS in Remote Clinic v2.0 in /medicines due to Medicine Name Field.	5.4	More Details
CVE-2021-2315	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data as well as unauthorized read access to a subset of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2021-21365	Bootstrap Package is a theme for TYPO3. It has been discovered that rendering content in the website frontend is vulnerable to cross-site scripting. A valid backend user account is needed to exploit this vulnerability. Users of the extension, who have overwritten the affected templates with custom code must manually apply the security fix. Update to version 7.1.2, 8.0.8, 9.1.4, 10.0.10 or 11.0.3 of the Bootstrap Package that fix the problem described. Updated version are available from the TYPO3 extension manager, Packagist and at https://extensions.typo3.org/extension/download/bootstrap_package/.	5.4	More Details
CVE-2020-17542	Cross Site Scripting (XSS) in dotCMS v5.1.5 allows remote attackers to execute arbitrary code by injecting a malicious payload into the "Task Detail" comment window of the "/dotAdmin/#/c/workflow" component.	5.4	More Details
CVE-2021-30635	Sonatype Nexus Repository Manager 3.x before 3.30.1 allows a remote attacker to get a list of files and directories that exist in a UI-related folder via directory traversal (no customer-specific data is exposed).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0273	An always-incorrect control flow implementation in the implicit filter terms of Juniper Networks Junos OS and Junos OS Evolved on ACX5800, EX9200 Series, MX10000 Series, MX240, MX480, MX960 devices with affected Trio line cards allows an attacker to exploit an interdependency in the PFE UCODE microcode of the Trio chipset with various line cards to cause packets destined to the devices interfaces to cause a Denial of Service (DoS) condition by looping the packet with an unreachable exit condition ('Infinite Loop'). To break this loop once it begins one side of the affected LT interfaces will need to be disabled. Once disabled, the condition will clear and the disabled LT interface can be reenabled. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue only affects LT-LT interfaces. Any other interfaces are not affected by this issue. This issue affects the following cards: MPCE Type 3 3D MPC4E 3D 32XGE MPC4E 3D 2CGE+8XGE EX9200 32x10G SFP EX9200-2C-8XS FPC Type 5-3D FPC Type 5-LSR EX9200 4x40G QSFP An Indicator of Compromise (IoC) can be seen by examining the traffic of the LT-LT interfaces for excessive traffic using the following command: monitor interface traffic Before loop impact: Interface: lt-2/0/0, Enabled, Link is Up Encapsulation: Logical-tunnel, Speed: 100000mbps Traffic statistics: Current delta Input bytes: 3759900268942 (1456 bps) [0] <---------- LT interface utilization is low Output bytes: 3759900344309 (1456 bps) [0] <---------- LT interface utilization is low After loop impact: Interface: lt-2/0/0, Enabled, Link is Up Encapsulation: Logical-tunnel, Speed: 100000mbps Traffic statistics: Current delta Input bytes: 3765160313129 (2158268368 bps) [5260044187] <---------- LT interface utilization is very high Output bytes: 3765160399522 (2158266440 bps) [5260055213] <---------- LT interface utilization is very high This issue affects: Juniper Networks Junos OS on ACX5800, EX9200 Series, MX10000 Series, MX240, MX480, MX960. Versions 15.1F6, 16.1R1, and later versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. This issue does not affect the MX10001. This issue does not affect Juniper Networks Junos OS versions prior to 15.1F6, 16.1R1. Juniper Networks Junos OS Evolved on ACX5800, EX9200 Series, MX10000 Series, MX240, MX480, MX960 19.4 versions prior to 19.4R2-EVO. This issue does not affect the MX10001.	5.3	More Details
CVE-2021-2234	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N).	5.3	More Details
CVE-2021-28399	OrangeHRM 4.7 allows an unauthenticated user to enumerate the valid username and email address via the forgot password function.	5.3	More Details
CVE-2020-4562	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information by allowing cross-window communication with unrestricted target origin via documentation frames.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2296	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	5.3	More Details
CVE-2021-31545	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The page_recent_contributors leaked the existence of certain deleted MediaWiki usernames, related to rev_deleted.	5.3	More Details
CVE-2021-2204	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2021-2163	Vulnerability in the Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u291, 8u281, 11.0.10, 16; Java SE Embedded: 8u281; Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2 and 21.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N).	5.3	More Details
CVE-2021-23382	The package postcss before 8.2.13 are vulnerable to Regular Expression Denial of Service (ReDoS) via getAnnotationURL() and loadAnnotation() in lib/previous-map.js. The vulnerable regexes are caused mainly by the sub-pattern \/*\s* sourceMappingURL=(.*).	5.3	More Details
CVE-2021-27393	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2013.08), Nucleus Source Code (Versions including affected DNS modules). The DNS client does not properly randomize UDP port numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving.	5.3	More Details
CVE-2021-20712	Improper access control vulnerability in NEC Aterm WG2600HS firmware Ver1.5.1 and earlier, and Aterm WX3000HP firmware Ver1.1.2 and earlier allows a device connected to the LAN side to be accessed from the WAN side due to the defect in the IPv6 firewall function.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0229	An uncontrolled resource consumption vulnerability in Message Queue Telemetry Transport (MQTT) server of Juniper Networks Junos OS allows an attacker to cause MQTT server to crash and restart leading to a Denial of Service (DoS) by sending a stream of specific packets. A Juniper Extension Toolkit (JET) application designed with a listening port uses the Message Queue Telemetry Transport (MQTT) protocol to connect to a mosquitto broker that is running on Junos OS to subscribe for events. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 16.1R1 and later versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.	5.3	More Details
CVE-2021-2297	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	5.3	More Details
CVE-2021-29469	Node-redis is a Node.js Redis client. Before version 3.1.1, when a client is in monitoring mode, the regex begin used to detected monitor messages could cause exponential backtracking on some strings. This issue could lead to a denial of service. The issue is patched in version 3.1.1.	5.3	More Details
CVE-2021-25677	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.3), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (Versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0 < V1.0.0.0), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving.	5.3	More Details
CVE-2020-25243	A vulnerability has been identified in LOGO! Soft Comfort (All versions < V8.4). A zip slip vulnerability could be triggered while importing a compromised project file to the affected software. Chained with other vulnerabilities this vulnerability could ultimately lead to a system takeover by an attacker.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0247	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: __default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.	5.1	More Details
CVE-2021-2212	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2194	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2217	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2215	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2213	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-29158	Sonatype Nexus Repository Manager 3 Pro up to and including 3.30.0 has Incorrect Access Control.	4.9	More Details
CVE-2021-2208	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2203	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2201	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2196	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2193	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2230	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2180	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2179	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2170	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2169	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2166	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2164	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2160	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2154	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2146	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2226	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2021-2293	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2278	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2299	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2300	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2305	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2303	Vulnerability in the OSS Support Tools product of Oracle Support Tools (component: Diagnostic Assistant). The supported version that is affected is Prior to 2.12.41. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise OSS Support Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all OSS Support Tools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2021-23365	The package github.com/tyktechnologies/tyk-identity-broker before 1.1.1 are vulnerable to Authentication Bypass via the Go XML parser which can cause SAML authentication bypass. This is because the XML parser doesn't guarantee integrity in the XML round-trip (encoding/decoding XML data).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29474	HedgeDoc (formerly known as CodiMD) is an open-source collaborative markdown editor. An attacker can read arbitrary `.md` files from the server's filesystem due to an improper input validation, which results in the ability to perform a relative path traversal. To verify if you are affected, you can try to open the following URL: `http://localhost:3000/..%2F..%2FREADME#` (replace `http://localhost:3000` with your instance's base-URL e.g. `https://demo.hedgedoc.org/..%2F..%2FREADME#`). If you see a README page being rendered, you run an affected version. The attack works due the fact that the internal router passes the url-encoded alias to the `noteController.showNote`-function. This function passes the input directly to findNote() utility function, that will pass it on the the parseNoteId()-function, that tries to make sense out of the noteId/alias and check if a note already exists and if so, if a corresponding file on disk was updated. If no note exists the note creation-function is called, which pass this unvalidated alias, with a `.md` appended, into a path.join()-function which is read from the filesystem in the follow up routine and provides the pre-filled content of the new note. This allows an attacker to not only read arbitrary `.md` files from the filesystem, but also observes changes to them. The usefulness of this attack can be considered limited, since mainly markdown files are use the file-ending `.md` and all markdown files contained in the hedgedoc project, like the README, are public anyway. If other protections such as a chroot or container or proper file permissions are in place, this attack's usefulness is rather limited. On a reverse-proxy level one can force a URL-decode, which will prevent this attack because the router will not accept such a path.	4.7	More Details
CVE-2021-29470	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.4.	4.7	More Details
CVE-2021-0243	Improper Handling of Unexpected Data in the firewall policer of Juniper Networks Junos OS on EX4300 switches allows matching traffic to exceed set policer limits, possibly leading to a limited Denial of Service (DoS) condition. When the firewall policer discard action fails on a Layer 2 port, it will allow traffic to pass even though it exceeds set policer limits. Traffic will not get discarded, and will be forwarded even though a policer discard action is configured. When the issue occurs, traffic is not discarded as desired, which can be observed by comparing the Input bytes with the Output bytes using the following command: user@junos> monitor interface traffic Interface Link Input bytes (bps) Output bytes (bps) ge-0/0/0 Up 37425422 (82616) 37425354 (82616) <<<< egress ge-0/0/1 Up 37425898 (82616) 37425354 (82616) <<<< ingress The expected output, with input and output counters differing, is shown below: Interface Link Input bytes (bps) Output bytes (bps) ge-0/0/0 Up 342420570 (54600) 342422760 (54600) <<<< egress ge-0/0/1 Up 517672120 (84000) 342420570 (54600) <<<< ingress This issue only affects IPv4 policing. IPv6 traffic and firewall policing actions are not affected by this issue. This issue affects Juniper Networks Junos OS on the EX4300: All versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2291	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	4.7	More Details
CVE-2021-2171	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2312	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2174	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2214	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.4	More Details
CVE-2021-2162	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2155	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2021-21645	Jenkins Config File Provider Plugin 3.7.0 and earlier does not perform permission checks in several HTTP endpoints, attackers with Overall/Read permission to enumerate configuration file IDs.	4.3	More Details
CVE-2021-21647	Jenkins CloudBees CD Plugin 1.1.21 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Item/Read permission to schedule builds of projects without having Item/Build permission.	4.3	More Details
CVE-2021-31549	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The Special:AbuseFilter/examine form allowed for the disclosure of suppressed MediaWiki usernames to unprivileged users.	4.3	More Details
CVE-2021-31547	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. Its AbuseFilterCheckMatch API reveals suppressed edits and usernames to unprivileged users through the iteration of crafted AbuseFilter rules.	4.3	More Details
CVE-2021-31546	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly logged sensitive suppression deletions, which should not have been visible to users with access to view AbuseFilter log data.	4.3	More Details
CVE-2021-2153	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Internet Expenses. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Internet Expenses accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2021-20715	Improper access control vulnerability in Hot Pepper Gourmet App for Android ver.4.111.0 and earlier, and for iOS ver.4.111.0 and earlier allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	4.3	More Details
CVE-2021-2173	Vulnerability in the Recovery component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA Level Account privilege with network access via Oracle Net to compromise Recovery. While the vulnerability is in Recovery, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Recovery accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2257	Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Storage Cloud Software Appliance accessible data. Note: Updating the Oracle Storage Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download the latest version of Oracle Storage Cloud Software Appliance from <a href=" https://www.oracle.com/downloads/cloud/oscsa-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rstype=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	4.1	More Details
CVE-2021-31404	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.13 (Vaadin 10.0.0 through 10.0.16), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.4.6 (Vaadin 14.0.0 through 14.4.6), 3.0.0 prior to 5.0.0 (Vaadin 15 prior to 18), and 5.0.0 through 5.0.2 (Vaadin 18.0.0 through 18.0.5) allows attacker to guess a security token via timing attack.	4.0	More Details
CVE-2021-2152	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N).	4.0	More Details
CVE-2021-21429	OpenAPI Generator allows generation of API client libraries, server stubs, documentation and configuration automatically given an OpenAPI Spec. Using `File.createTempFile` in JDK will result in creating and using insecure temporary files that can leave application and system data vulnerable to attacks. OpenAPI Generator maven plug-in creates insecure temporary files during the process. The issue has been patched with `Files.createTempFile` and released in the v5.1.0 stable version.	4.0	More Details
CVE-2021-31403	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:vaadin-server versions 7.0.0 through 7.7.23 (Vaadin 7.0.0 through 7.7.23), and 8.0.0 through 8.12.2 (Vaadin 8.0.0 through 8.12.2) allows attacker to guess a security token via timing attack	4.0	More Details
CVE-2021-31406	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server versions 3.0.0 through 5.0.3 (Vaadin 15.0.0 through 18.0.6), and com.vaadin:fusion-endpoint version 6.0.0 (Vaadin 19.0.0) allows attacker to guess a security token for Fusion endpoints via timing attack.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2158	Vulnerability in the Hyperion Financial Management product of Oracle Hyperion (component: Task Automation). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion Financial Management. CVSS 3.1 Base Score 3.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L).	3.9	More Details
CVE-2021-24242	The Tutor LMS – eLearning and online course solution WordPress plugin before 1.8.8 is affected by a local file inclusion vulnerability through the maliciously constructed sub_page parameter of the plugin's Tools, allowing high privilege users to include any local php file	3.8	More Details
CVE-2021-26909	Automox Agent prior to version 31 uses an insufficiently protected S3 bucket endpoint for storing sensitive files, which could be brute-forced by an attacker to subvert an organization's security program. The issue has since been fixed in version 31 of the Automox Agent.	3.7	More Details
CVE-2021-22199	An issue has been discovered in GitLab affecting all versions starting with 12.9. GitLab was vulnerable to a stored XSS if scoped labels were used.	3.5	More Details
CVE-2021-2159	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Frameworks). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 3.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).	3.5	More Details
CVE-2021-26908	Automox Agent prior to version 31 logs potentially sensitive information in local log files, which could be used by a locally-authenticated attacker to subvert an organization's security program. The issue has since been fixed in version 31 of the Automox Agent.	3.3	More Details
CVE-2020-36319	Insecure configuration of default ObjectMapper in com.vaadin:flow-server versions 3.0.0 through 3.0.5 (Vaadin 15.0.0 through 15.0.4) may expose sensitive data if the application also uses e.g. @RestController	3.1	More Details
CVE-2021-2245	Vulnerability in the Oracle Database - Enterprise Edition Unified Audit component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Audit Policy privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Unified Audit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Unified Audit accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2175	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any View, Select Any View privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.7	More Details
CVE-2021-2308	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.7	More Details
CVE-2021-2301	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.7	More Details
CVE-2018-25007	Missing check in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.5 (Vaadin 10.0.0 through 10.0.7, and 11.0.0 through 11.0.2) allows attacker to update element property values via crafted synchronization message.	2.6	More Details
CVE-2021-2149	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	2.5	More Details
CVE-2021-29473	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4. Please see our security policy for information about Exiv2 security.	2.5	More Details
CVE-2021-2207	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having RMAN executable privilege with logon to the infrastructure where Oracle Database - Enterprise Edition executes to compromise Oracle Database - Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2141	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.2 and 12.0.3. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 2.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	2.0	More Details
CVE-2021-2232	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	1.9	More Details
CVE-2021-2147	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Installation). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	1.8	More Details
CVE-2021-30031	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2017-20003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details