SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 May 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-2021-20716	Hidden functionality in multiple Buffalo network devices (BHR-4RV firmware Ver.2.55 and prior, FS-G54 firmware Ver.2.04 and prior, WBR2-B11 firmware Ver.2.32 and prior, WBR2-G54 firmware Ver.2.32 and prior, WBR2-G54-KD firmware Ver.2.32 and prior, WBR-B11 firmware Ver.2.23 and prior, WBR-G54 firmware Ver.2.23 and prior, WBR-G54L firmware Ver.2.20 and prior, WHR2-A54G54 firmware Ver.2.25 and prior, WHR2-G54 firmware Ver.2.23 and prior, WHR2-G54V firmware Ver.2.55 and prior, WHR3-AG54 firmware Ver.2.23 and prior, WHR-G54 firmware Ver.2.16 and prior, WHR-G54-NF firmware Ver.2.10 and prior, WLA2-G54 firmware Ver.2.24 and prior, WLA2-G54C firmware Ver.2.24 and prior, WLA-B11 firmware Ver.2.20 and prior, WLA-G54 firmware Ver.2.20 and prior, WLA-G54C firmware Ver.2.20 and prior, WLAH-A54G54 firmware Ver.2.54 and prior, WLAH-AM54G54 firmware Ver.2.54 and prior, WLAH-G54 firmware Ver.2.54 and prior, WLI2-TX1-AG54 firmware Ver.2.53 and prior, WLI2-TX1-AMG54 firmware Ver.2.53 and prior, WLI2-TX1-G54 firmware Ver.2.20 and prior, WLI3-TX1-AMG54 firmware Ver.2.53 and prior, WLI3-TX1-G54 firmware Ver.2.53 and prior, WLI-T1-B11 firmware Ver.2.20 and prior, WLI-TX1-G54 firmware Ver.2.20 and prior, WVR-G54-NF firmware Ver.2.02 and prior, WZR-G108 firmware Ver.2.41 and prior, WZR-G54 firmware Ver.2.41 and prior, WZR-HP-G54 firmware Ver.2.41 and prior, WZR-RS-G54 firmware Ver.2.55 and prior, and WZR-RS-G54HP firmware Ver.2.55 and prior) allows a remote attacker to enable the debug option and to execute arbitrary code or OS commands, change the configuration, and cause a denial of service (DoS) condition.	9.8	More Details
CVE-2021-30230	The api/ZRFirmware/set_time_zone interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the zonename parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30232	The api/ZRIGMP/set_IGMP_PROXY interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the IGMP_PROXY_WAN_CONNECT parameter.	9.8	More Details
CVE-2021-30233	The api/ZRIptv/setIptvInfo interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the iptv_vlan parameter.	9.8	More Details
CVE-2021-30234	The api/ZRIGMP/set_MLD_PROXY interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the MLD_PROXY_WAN_CONNECT parameter.	9.8	More Details
CVE-2020-21452	An issue was discovered in uniview ISC2500-S. This is an upload vulnerability where an attacker can upload malicious code via /Interface/DevManage/EC.php?cmd=upload	9.8	More Details
CVE-2020-35430	SQL Injection in com/inxedu/OS/edu/controller/letter/AdminMsgSystemController in Inxedu v2.0.6 via the ids parameter to admin/letter/delsystem.	9.8	More Details
CVE-2020-22807	An issue was dicovered in vtiger crm 7.2. Union sql injection in the calendar exportdata feature.	9.8	More Details
CVE-2021-31870	An issue was discovered in klibc before 2.0.9. Multiplication in the calloc() function may result in an integer overflow and a subsequent heap buffer overflow.	9.8	More Details
CVE-2021-31872	An issue was discovered in klibc before 2.0.9. Multiple possible integer overflows in the cpio command on 32-bit systems may result in a buffer overflow or other security impact.	9.8	More Details
CVE-2021-31873	An issue was discovered in klibc before 2.0.9. Additions in the malloc() function may result in an integer overflow and a subsequent heap buffer overflow.	9.8	More Details
CVE-2020-24918	A buffer overflow in the RTSP service of the Ambarella Oryx RTSP Server 2020-01-07 allows an unauthenticated attacker to send a crafted RTSP request, with a long digest authentication header, to execute arbitrary code in parse_authentication_header() in libamprotocol-rtsp.so.1 in rtsp_svc (or cause a crash). This allows remote takeover of a Furbo Dog Camera, for example. NOTE: The vendor states that the RTSP library is used for DEMO only, using it in product is a customer's behavior. Ambarella has emphasized that RTSP is DEMO only library, should NOT be used in product in our document. Because Ambarella's SDK is proprietary, we didn't publish our SDK source code in public network.	9.8	More Details
CVE-2021-28959	Zoho ManageEngine Eventlog Analyzer through 12147 is vulnerable to unauthenticated directory traversal via an entry in a ZIP archive. This leads to remote code execution.	9.8	More Details
CVE-2021-29369	The gnuplot package prior to version 0.1.0 for Node.js allows code execution via shell metacharacters in Gnuplot commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35757	An issue was discovered on Libre Wireless LS9 LS1.5/p7040 devices. There is Unauthenticated Root ADB Access Over TCP. The LS9 web interface provides functionality to access ADB over TCP. This is not enabled by default, but can be enabled by sending a crafted request to a web management interface endpoint. Requests made to this endpoint do not require authentication. As such, any unauthenticated user who is able to access the web interface will be able to gain root privileges on the LS9 module.	9.8	More Details
CVE-2020-35758	An issue was discovered on Libre Wireless LS9 LS1.5/p7040 devices. There is a Authentication Bypass in the Web Interface. This interface does not properly restrict access to internal functionality. Despite presenting a password login page on first access, authentication is not required to access privileged functionality. As such, it's possible to directly access APIs that should not be exposed to an unauthenticated user.	9.8	More Details
CVE-2020-23083	Unrestricted File Upload in JEECG v4.0 and earlier allows remote attackers to execute arbitrary code or gain privileges by uploading a crafted file to the component "jeecgFormDemoController.do?commonUpload".	9.8	More Details
CVE-2020-36326	PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation.	9.8	More Details
CVE-2021-30231	The api/zrDm/set_ZRElink interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the bssaddr, abiaddr, devtoken, devid, elinksync, or elink_proc_enable parameter.	9.8	More Details
CVE-2021-30228	The api/ZRAndlink/set_ZRAndlink interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the iandlink_proc_enable parameter.	9.8	More Details
CVE-2021-25812	Command injection vulnerability in China Mobile An Lianbao WF-1 1.01 via the 'ip' parameter with a POST request to /api/ZRQos/set_online_client.	9.8	More Details
CVE-2021-31856	A SQL Injection vulnerability in the REST API in Layer5 Meshery 0.5.2 allows an attacker to execute arbitrary SQL commands via the /experimental/patternfiles endpoint (order parameter in GetMesheryPatterns in models/meshery_pattern_persister.go).	9.8	More Details
CVE-2021-30167	The manage users profile services of the network camera device allows an authenticated. Remote attackers can modify URL parameters and further amend user’s information and escalate privileges to control the devices.	9.8	More Details
CVE-2021-30168	The sensitive information of webcam device is not properly protected. Remote attackers can unauthentically grant administrator’s credential and further control the devices.	9.8	More Details
CVE-2021-22514	An arbitrary code execution vulnerability exists in Micro Focus Application Performance Management, affecting versions 9.40, 9.50 and 9.51. The vulnerability could allow remote attackers to execute arbitrary code on affected installations of APM.	9.8	More Details
CVE-2020-18020	SQL Injection in PHPSHE Mall System v1.7 allows remote attackers to execute arbitrary code by injecting SQL commands into the "user_phone" parameter of a crafted HTTP request to the "admin.php" component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21991	AVE DOMINAplus <=1.10.x suffers from an authentication bypass vulnerability due to missing control check when directly calling the autologin GET parameter in changeparams.php script. Setting the autologin value to 1 allows an unauthenticated attacker to permanently disable the authentication security control and access the management interface with admin privileges without providing credentials.	9.8	More Details
CVE-2020-21994	AVE DOMINAplus <=1.10.x suffers from clear-text credentials disclosure vulnerability that allows an unauthenticated attacker to issue a request to an unprotected directory that hosts an XML file '/xml/authClients.xml' and obtain administrative login information that allows for a successful authentication bypass attack.	9.8	More Details
CVE-2021-31875	In mjs_json.c in Cesanta MongooseOS mJS 1.26, a maliciously formed JSON string can trigger an off-by-one heap-based buffer overflow in mjs_json_parse, which can potentially lead to redirection of control flow. NOTE: the original reporter disputes the significance of this finding because "there isn't very much of an opportunity to exploit this reliably for an information leak, so there isn't any real security impact."	9.8	More Details
CVE-2021-29145	A remote server side request forgery (SSRF) remote code execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	9.8	More Details
CVE-2020-21995	Inim Electronics Smartliving SmartLAN/G/SI <=6.x uses default hardcoded credentials. An attacker could exploit this to gain Telnet, SSH and FTP access to the system.	9.8	More Details
CVE-2021-20090	A path traversal vulnerability in the web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 could allow unauthenticated remote attackers to bypass authentication.	9.8	More Details
CVE-2021-27651	In versions 8.2.1 through 8.5.2 of Pega Infinity, the password reset functionality for local accounts can be used to bypass local authentication checks.	9.8	More Details
CVE-2021-32020	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has insufficient bounds checking during management of heap memory.	9.8	More Details
CVE-2021-29483	ManageWiki is an extension to the MediaWiki project. The 'wikiconfig' API leaked the value of private configuration variables set through the ManageWiki variable to all users. This has been patched by https://github.com/miraheze/ManageWiki/compare/99f3b2c8af18...befb83c66f5b.patch. If you are unable to patch set `$wgAPIListModules['wikiconfig'] = 'ApiQueryDisabled';` or remove private config as a workaround.	9.4	More Details
CVE-2020-18070	Path Traversal in iCMS v7.0.13 allows remote attackers to delete folders by injecting commands into a crafted HTTP request to the "do_del()" method of the component "database.admincp.php".	9.1	More Details
CVE-2021-28860	In Node.js mixme, prior to v0.5.1, an attacker can add or alter properties of an object via '__proto__' through the mutate() and merge() functions. The polluted attribute will be directly assigned to every object in the program. This will put the availability of the program at risk causing a potential denial of service (DoS).	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27648	Externally controlled reference to a resource in another sphere in quarantine functionality in Synology Antivirus Essential before 1.4.8-2801 allows remote authenticated users to obtain privilege via unspecified vectors.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-21388	systeminformation is an open source system and OS information library for node.js. A command injection vulnerability has been discovered in versions of systeminformation prior to 5.6.4. The issue has been fixed with a parameter check on user input. Please upgrade to version >= 5.6.4. If you cannot upgrade, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() and other commands. Only allow strings, reject any arrays. String sanitation works as expected.	8.9	More Details
CVE-2021-29147	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	8.8	More Details
CVE-2021-29238	CODESYS Automation Server before 1.16.0 allows cross-site request forgery (CSRF).	8.8	More Details
CVE-2021-31425	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.2-49151. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Parallels Tools component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel on the target guest system. Was ZDI-CAN-12790.	8.8	More Details
CVE-2021-25631	In the LibreOffice 7-1 series in versions prior to 7.1.2, and in the 7-0 series in versions prior to 7.0.5, the denylist can be circumvented by manipulating the link so it doesn't match the denylist but results in ShellExecute attempting to launch an executable type.	8.8	More Details
CVE-2021-31424	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Open Tools Gate component. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12848.	8.8	More Details
CVE-2021-21227	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 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-2021-31420	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.0-48950. An attacker must first obtain the ability to execute low-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 the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12220.	8.8	More Details
CVE-2021-29468	Cygwin Git is a patch set for the git command line tool for the cygwin environment. A specially crafted repository that contains symbolic links as well as files with backslash characters in the file name may cause just-checked out code to be executed while checking out a repository using Git on Cygwin. The problem will be patched in the Cygwin Git v2.31.1-2 release. At time of writing, the vulnerability is present in the upstream Git source code; any Cygwin user who compiles Git for themselves from upstream sources should manually apply a patch to mitigate the vulnerability. As mitigation users should not clone or pull from repositories from untrusted sources. CVE-2019-1354 was an equivalent vulnerability in Git for Visual Studio.	8.8	More Details
CVE-2021-30229	The api/zrDm/set_zrDm interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the dm_enable, AppKey, or Pwd parameter.	8.8	More Details
CVE-2021-30224	Cross Site Request Forgery (CSRF) in Rukovoditel v2.8.3 allows attackers to create an admin user with an arbitrary credentials.	8.8	More Details
CVE-2021-21507	Dell EMC Networking X-Series firmware versions prior to 3.0.1.8 and Dell EMC PowerEdge VRTX Switch Module firmware versions prior to 2.0.0.82 contain a Weak Password Encryption Vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable system with privileges of the compromised account.	8.8	More Details
CVE-2021-21233	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21232	Use after free in Dev Tools in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-20091	The web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 do not properly sanitize user input. An authenticated remote attacker could leverage this vulnerability to alter device configuration, potentially gaining remote code execution.	8.8	More Details
CVE-2020-21992	Inim Electronics SmartLiving SmartLAN/G/SI <=6.x suffers from an authenticated remote command injection vulnerability. The issue exist due to the 'par' POST parameter not being sanitized when called with the 'testemail' module through web.cgi binary. The vulnerable CGI binary (ELF 32-bit LSB executable, ARM) is calling the 'sh' executable via the system() function to issue a command using the mailx service and its vulnerable string format parameter allowing for OS command injection with root privileges. An attacker can remotely execute system commands as the root user using default credentials and bypass access controls in place.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36327	Bundler 1.16.0 through 2.2.9 and 2.2.11 through 2.2.16 sometimes chooses a dependency source based on the highest gem version number, which means that a rogue gem found at a public source may be chosen, even if the intended choice was a private gem that is a dependency of another private gem that is explicitly depended on by the application. NOTE: it is not correct to use CVE-2021-24105 for every "Dependency Confusion" issue in every product.	8.8	More Details
CVE-2021-21231	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-25166	A remote unauthorized access vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.8	More Details
CVE-2021-25167	A remote unauthorized access vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.8	More Details
CVE-2021-21230	Type confusion in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-31426	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.2-49151. 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 Parallels Tools component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel on the target guest system. Was ZDI-CAN-12791.	8.8	More Details
CVE-2021-25151	A remote insecure deserialization vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.8	More Details
CVE-2021-21551	Dell dbutil_2_3.sys driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required.	8.8	More Details
CVE-2020-21999	iWT Ltd FaceSentry Access Control System 6.4.8 suffers from an authenticated OS command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user via the 'strInIP' POST parameter in pingTest PHP script.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3512	Improper access control vulnerability in Buffalo broadband routers (BHR-4GRV firmware Ver.1.99 and prior, DWR-HP-G300NH firmware Ver.1.83 and prior, HW-450HP-ZWE firmware Ver.1.99 and prior, WHR-300HP firmware Ver.1.99 and prior, WHR-300 firmware Ver.1.99 and prior, WHR-G301N firmware Ver.1.86 and prior, WHR-HP-G300N firmware Ver.1.99 and prior, WHR-HP-GN firmware Ver.1.86 and prior, WPL-05G300 firmware Ver.1.87 and prior, WZR-450HP-CWT firmware Ver.1.99 and prior, WZR-450HP-UB firmware Ver.1.99 and prior, WZR-HP-AG300H firmware Ver.1.75 and prior, WZR-HP-G300NH firmware Ver.1.83 and prior, WZR-HP-G301NH firmware Ver.1.83 and prior, WZR-HP-G302H firmware Ver.1.85 and prior, WZR-HP-G450H firmware Ver.1.89 and prior, WZR-300HP firmware Ver.1.99 and prior, WZR-450HP firmware Ver.1.99 and prior, WZR-600DHP firmware Ver.1.99 and prior, WZR-D1100H firmware Ver.1.99 and prior, FS-HP-G300N firmware Ver.3.32 and prior, FS-600DHP firmware Ver.3.38 and prior, FS-R600DHP firmware Ver.3.39 and prior, and FS-G300N firmware Ver.3.13 and prior) allows remote unauthenticated attackers to bypass access restriction and to start telnet service and execute arbitrary OS commands with root privileges via unspecified vectors.	8.8	More Details
CVE-2021-1445	Multiple vulnerabilities in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to lack of proper input validation of the HTTPS request. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	8.6	More Details
CVE-2021-1402	A vulnerability in the software-based SSL/TLS message handler of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message through an affected device. SSL/TLS messages sent to an affected device do not trigger this vulnerability. A successful exploit could allow the attacker to cause a process to crash. This crash would then trigger a reload of the device. No manual intervention is needed to recover the device after the reload.	8.6	More Details
CVE-2020-4039	SUSI.AI is an intelligent Open Source personal assistant. SUSI.AI Server before version d27ed0f has a directory traversal vulnerability due to insufficient input validation. Any admin config and file readable by the app can be retrieved by the attacker. Furthermore, some files can also be moved or deleted.	8.6	More Details
CVE-2021-1504	Multiple vulnerabilities in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to lack of proper input validation of the HTTPS request. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1501	A vulnerability in the SIP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a crash and reload of an affected device, resulting in a denial of service (DoS) condition.The vulnerability is due to a crash that occurs during a hash lookup for a SIP pinhole connection. An attacker could exploit this vulnerability by sending crafted SIP traffic through an affected device. A successful exploit could allow the attacker to cause a crash and reload of the affected device.	8.6	More Details
CVE-2021-1493	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a buffer overflow on an affected system. The vulnerability is due to insufficient boundary checks for specific data that is provided to the web services interface of an affected system. An attacker could exploit this vulnerability by sending a malicious HTTP request. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system, which could disclose data fragments or cause the device to reload, resulting in a denial of service (DoS) condition.	8.5	More Details
CVE-2021-21530	Dell OpenManage Enterprise-Modular (OME-M) versions prior to 1.30.00 contain a security bypass vulnerability. An authenticated malicious user with low privileges may potentially exploit the vulnerability to escape from the restricted environment and gain access to sensitive information in the system, resulting in information disclosure and elevation of privilege.	8.3	More Details
CVE-2021-31428	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.5-47309. 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 IDE virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13186.	8.2	More Details
CVE-2021-29140	A remote XML external entity (XXE) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	8.2	More Details
CVE-2021-31429	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.5-47309. 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 IDE virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13187.	8.2	More Details
CVE-2020-15153	Ampache before version 4.2.2 allows unauthenticated users to perform SQL injection. Refer to the referenced GitHub Security Advisory for details and a workaround. This is fixed in version 4.2.2 and the development branch.	8.2	More Details
CVE-2021-25165	A remote XML external entity vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25216	In BIND 9.5.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.11.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch, BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting values for the tkey-gssapi-keytab or tkey-gssapi-credential configuration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. For servers that meet these conditions, the ISC SPNEGO implementation is vulnerable to various attacks, depending on the CPU architecture for which BIND was built: For named binaries compiled for 64-bit platforms, this flaw can be used to trigger a buffer over-read, leading to a server crash. For named binaries compiled for 32-bit platforms, this flaw can be used to trigger a server crash due to a buffer overflow and possibly also to achieve remote code execution. We have determined that standard SPNEGO implementations are available in the MIT and Heimdal Kerberos libraries, which support a broad range of operating systems, rendering the ISC implementation unnecessary and obsolete. Therefore, to reduce the attack surface for BIND users, we will be removing the ISC SPNEGO implementation in the April releases of BIND 9.11 and 9.16 (it had already been dropped from BIND 9.17). We would not normally remove something from a stable ESV (Extended Support Version) of BIND, but since system libraries can replace the ISC SPNEGO implementation, we have made an exception in this case for reasons of stability and security.	8.1	More Details
CVE-2021-25153	A remote SQL injection vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.1	More Details
CVE-2021-25163	A remote XML external entity vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.1	More Details
CVE-2021-25147	A remote authentication restriction bypass vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	8.1	More Details
CVE-2021-21531	Dell Unisphere for PowerMax versions prior to 9.2.1.6 contain an Authorization Bypass Vulnerability. A local authenticated malicious user with monitor role may exploit this vulnerability to perform unauthorized actions.	8.1	More Details
CVE-2020-7037	An XML External Entities (XXE) vulnerability in Media Server component of Avaya Equinox Conferencing could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system or even potentially lead to a denial of service. The affected versions of Avaya Equinox Conferencing includes all 9.x versions before 9.1.11. Equinox Conferencing is now offered as Avaya Meetings Server.	8.1	More Details
CVE-2020-18032	Buffer Overflow in Graphviz Graph Visualization Tools from commit ID f8b9e035 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by loading a crafted file into the "lib/common/shapes.c" component.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1448	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device that is running in multi-instance mode. This vulnerability is due to insufficient validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	7.8	More Details
CVE-2021-1082	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data, or denial of service. vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7)	7.8	More Details
CVE-2021-31438	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12443.	7.8	More Details
CVE-2021-26807	GalaxyClient version 2.0.28.9 loads unsigned DLLs such as zlib1.dll, libgcc_s_dw2-1.dll and libwinpthread-1.dll from PATH, which allows an attacker to potentially run code locally through unsigned DLL loading.	7.8	More Details
CVE-2021-31437	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12384.	7.8	More Details
CVE-2021-20294	A flaw was found in binutils readelf 2.35 program. An attacker who is able to convince a victim using readelf to read a crafted file could trigger a stack buffer overflow, out-of-bounds write of arbitrary data supplied by the attacker. The highest impact of this flaw is to confidentiality, integrity, and availability.	7.8	More Details
CVE-2021-31436	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of SGI files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12376.	7.8	More Details
CVE-2021-21415	Prisma VS Code a VSCode extension for Prisma schema files. This is a Remote Code Execution Vulnerability that affects all versions of the Prisma VS Code extension older than 2.20.0. If a custom binary path for the Prisma format binary is set in VS Code Settings, for example by downloading a project that has a .vscode/settings.json file that sets a value for "prismaFmtBinPath". That custom binary is executed when auto-formatting is triggered by VS Code or when validation checks are triggered after each keypress on a *.prisma file. Fixed in versions 2.20.0 and 20.0.27. As a workaround users can either edit or delete the `.vscode/settings.json` file or check if the binary is malicious and delete it.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31435	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CMP files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12331.	7.8	More Details
CVE-2021-1084	NVIDIA vGPU driver contains a vulnerability in the guest kernel mode driver and Virtual GPU Manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data or denial of service. This affects vGPU version 12.x (prior to 12.2) and version 11.x (prior to 11.4).	7.8	More Details
CVE-2021-31433	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ARW files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12333.	7.8	More Details
CVE-2021-1083	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and Virtual GPU Manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data, or denial of service. This affects vGPU version 12.x (prior to 12.2) and version 11.x (prior to 11.4).	7.8	More Details
CVE-2021-1080	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), in which certain input data is not validated, which may lead to information disclosure, tampering of data, or denial of service. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior 8.7).	7.8	More Details
CVE-2021-1081	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and Virtual GPU manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data, or denial of service. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior 8.7).	7.8	More Details
CVE-2020-27519	Pritunl Client v1.2.2550.20 contains a local privilege escalation vulnerability in the pritunl-service component. The attack vector is: malicious openvpn config. A local attacker could leverage the log and log-append along with log injection to create or append to privileged script files and execute code as root/SYSTEM.	7.8	More Details
CVE-2021-31434	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12377.	7.8	More Details
CVE-2021-29239	CODESYS Development System 3 before 3.5.17.0 displays or executes malicious documents or files embedded in libraries without first checking their validity.	7.8	More Details
CVE-2020-27518	All versions of Windscribe VPN for Mac and Windows <= v2.02.10 contain a local privilege escalation vulnerability in the WindscribeService component. A low privilege user could leverage several openvpn options to execute code as root/SYSTEM.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31776	Aviatrix VPN Client before 2.14.14 on Windows has an unquoted search path that enables local privilege escalation to the SYSTEM user, if the machine is misconfigured to allow unprivileged users to write to directories that are supposed to be restricted to administrators.	7.8	More Details
CVE-2021-29240	The Package Manager of CODESYS Development System 3 before 3.5.17.0 does not check the validity of packages before installation and may be used to install CODESYS packages with malicious content.	7.8	More Details
CVE-2020-7123	A local escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	7.8	More Details
CVE-2021-21414	Prisma is an open source ORM for Node.js & TypeScript. As of today, we are not aware of any Prisma users or external consumers of the `@prisma/sdk` package who are affected by this security vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. It only affects the `getPackedPackage` function and this function is not advertised and only used for tests & building our CLI, no malicious code was found after checking our codebase.	7.7	More Details
CVE-2021-31863	Insufficient input validation in the Git repository integration of Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows Redmine users to read arbitrary local files accessible by the application server process.	7.5	More Details
CVE-2021-29482	xz is a compression and decompression library focusing on the xz format completely written in Go. The function readUvarint used to read the xz container format may not terminate a loop provide malicous input. The problem has been fixed in release v0.5.8. As a workaround users can limit the size of the compressed file input to a reasonable size for their use case. The standard library had recently the same issue and got the CVE-2020-16845 allocated.	7.5	More Details
CVE-2021-25154	A remote escalation of privilege vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	7.5	More Details
CVE-2021-31422	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 e1000e virtual device. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12527.	7.5	More Details
CVE-2020-28944	OX Guard 2.10.4 and earlier allows a Denial of Service via a WKS server that responds slowly or with a large amount of data.	7.5	More Details
CVE-2021-31996	An issue was discovered in the algorithmica crate through 2021-03-07 for Rust. There is a double free in merge_sort::merge().	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15225	django-filter is a generic system for filtering Django QuerySets based on user selections. In django-filter before version 2.4.0, automatically generated `NumberFilter` instances, whose value was later converted to an integer, were subject to potential DoS from maliciously input using exponential format with sufficiently large exponents. Version 2.4.0+ applies a `MaxValueValidator` with a a default `limit_value` of 1e50 to the form field used by `NumberFilter` instances. In addition, `NumberFilter` implements the new `get_max_validator()` which should return a configured validator instance to customise the limit, or else `None` to disable the additional validation. Users may manually apply an equivalent validator if they are not able to upgrade.	7.5	More Details
CVE-2020-21996	AVE DOMINAplus <=1.10.x suffers from an unauthenticated reboot command execution. Attackers can exploit this issue to cause a denial of service scenario.	7.5	More Details
CVE-2021-31871	An issue was discovered in klibc before 2.0.9. An integer overflow in the cpio command may result in a NULL pointer dereference on 64-bit systems.	7.5	More Details
CVE-2021-29241	CODESYS Gateway 3 before 3.5.16.70 has a NULL pointer dereference that may result in a denial of service (DoS).	7.5	More Details
CVE-2020-18019	SQL Injection in Xinhu OA System v1.8.3 allows remote attackers to obtain sensitive information by injecting arbitrary commands into the "typeid" variable of the "createfolderAjax" function in the "mode_worcAction.php" component.	7.5	More Details
CVE-2021-22332	There is a pointer double free vulnerability in some versions of CloudEngine 5800, CloudEngine 6800, CloudEngine 7800 and CloudEngine 12800. When a function is called, the same memory pointer is copied to two functional modules. Attackers can exploit this vulnerability by performing a malicious operation to cause the pointer double free. This may lead to module crash, compromising normal service.	7.5	More Details
CVE-2021-22331	There is a JavaScript injection vulnerability in certain Huawei smartphones. A module does not verify some inputs sufficiently. Attackers can exploit this vulnerability by sending a malicious application request to launch JavaScript injection. This may compromise normal service. Affected product versions include HUAWEI P30 versions earlier than 10.1.0.165(C01E165R2P11), 11.0.0.118(C635E2R1P3), 11.0.0.120(C00E120R2P5), 11.0.0.138(C10E4R5P3), 11.0.0.138(C185E4R7P3), 11.0.0.138(C432E8R2P3), 11.0.0.138(C461E4R3P3), 11.0.0.138(C605E4R1P3), and 11.0.0.138(C636E4R3P3).	7.5	More Details
CVE-2021-22393	There is a denial of service vulnerability in some versions of CloudEngine 5800, CloudEngine 6800, CloudEngine 7800 and CloudEngine 12800. The affected product cannot deal with some messages because of module design weakness . Attackers can exploit this vulnerability by sending a large amount of specific messages to cause denial of service. This can compromise normal service.	7.5	More Details
CVE-2021-31164	Apache Unomi prior to version 1.5.5 allows CRLF log injection because of the lack of escaping in the log statements.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35755	An issue was discovered on Libre Wireless LS9 LS1.5/p7040 devices. There is a luci_service Read_ NVRAM Direct Access Information Leak. The luci_service deamon running on port 7777 provides a sub-category of commands for which Read_ is prepended. Commands in this category are able to directly read the contents of the device configuration NVRAM. The NVRAM contains sensitive information, such as the Wi-Fi password (in cleartext), as well as connected account tokens for services such as Spotify.	7.5	More Details
CVE-2021-31919	An issue was discovered in the rkyv crate before 0.6.0 for Rust. When an archive is created via serialization, the archive content may contain uninitialized values of certain parts of a struct.	7.5	More Details
CVE-2020-22781	In Etherpad < 1.8.3, a specially crafted URI would raise an unhandled exception in the cache mechanism and cause a denial of service (crash the instance).	7.5	More Details
CVE-2020-7038	A vulnerability was discovered in Management component of Avaya Equinox Conferencing that could potentially allow an unauthenticated, remote attacker to gain access to screen sharing and whiteboard sessions. The affected versions of Management component of Avaya Equinox Conferencing include all 3.x versions before 3.17. Avaya Equinox Conferencing is now offered as Avaya Meetings Server.	7.5	More Details
CVE-2020-22785	Etherpad < 1.8.3 is affected by a missing lock check which could cause a denial of service. Aggressively targeting random pad import endpoints with empty data would flatten all pads due to lack of rate limiting and missing ownership check.	7.5	More Details
CVE-2021-29478	Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. An integer overflow bug in Redis 6.2 before 6.2.3 could be exploited to corrupt the heap and potentially result with remote code execution. Redis 6.0 and earlier are not directly affected by this issue. The problem is fixed in version 6.2.3. An additional workaround to mitigate the problem without patching the `redis-server` executable is to prevent users from modifying the `set-max-intset-entries` configuration parameter. This can be done using ACL to restrict unprivileged users from using the `CONFIG SET` command.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29486	cumulative-distribution-function is an open source npm library used which calculates statistical cumulative distribution function from data array of x values. In versions prior to 2.0.0 apps using this library on improper data may crash or go into an infinite-loop. In the case of a nodejs server-app using this library to act on invalid non-numeric data, the nodejs server may crash. This may affect other users of this server and/or require the server to be rebooted for proper operation. In the case of a browser app using this library to act on invalid non-numeric data, that browser may crash or lock up. A flaw enabling an infinite-loop was discovered in the code for evaluating the cumulative-distribution-function of input data. Although the documentation explains that numeric data is required, some users may confuse an array of strings like ["1","2","3","4","5"] for numeric data [1,2,3,4,5] when it is in fact string data. An infinite loop is possible when the cumulative-distribution-function is evaluated for a given point when the input data is string data rather than type `number`. This vulnerability enables an infinite-cpu-loop denial-of-service-attack on any app using npm:cumulative-distribution-function v1.0.3 or earlier if the attacker can supply malformed data to the library. The vulnerability could also manifest if a data source to be analyzed changes data type from Arrays of number (proper) to Arrays of string (invalid, but undetected by earlier version of the library). Users should upgrade to at least v2.0.0, or the latest version. Tests for several types of invalid data have been created, and version 2.0.0 has been tested to reject this invalid data by throwing a `TypeError()` instead of processing it. Developers using this library may wish to adjust their app's code slightly to better tolerate or handle this TypeError. Apps performing proper numeric data validation before sending data to this library should be mostly unaffected by this patch. The vulnerability can be mitigated in older versions by ensuring that only finite numeric data of type `Array[number]` or `number` is passed to `cumulative-distribution-function` and its `f(x)` function, respectively.	7.5	More Details
CVE-2020-21990	Emmanuel MyDomoAtHome (MDAH) REST API REST API Domoticz ISS Gateway 0.2.40 is affected by an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this, via a specially crafted request to gain access to sensitive information.	7.5	More Details
CVE-2021-29477	Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. An integer overflow bug in Redis version 6.0 or newer could be exploited using the `STRALGO LCS` command to corrupt the heap and potentially result with remote code execution. The problem is fixed in version 6.2.3 and 6.0.13. An additional workaround to mitigate the problem without patching the redis-server executable is to use ACL configuration to prevent clients from using the `STRALGO LCS` command.	7.5	More Details
CVE-2020-21997	Smartwares HOME easy <=1.0.9 is vulnerable to an unauthenticated database backup download and information disclosure vulnerability. An attacker could disclose sensitive and clear-text information resulting in authentication bypass, session hijacking and full system control.	7.5	More Details
CVE-2020-22002	An Unauthenticated Server-Side Request Forgery (SSRF) vulnerability exists in Inim Electronics Smartliving SmartLAN/G/SI <=6.x within the GetImage functionality. The application parses user supplied data in the GET parameter 'host' to construct an image request to the service through onvif.cgi. Since no validation is carried out on the parameter, an attacker can specify an external domain and force the application to make an HTTP request to an arbitrary destination host.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25215	In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a query for a record triggering the flaw described above, the named process will terminate due to a failed assertion check. The vulnerability affects all currently maintained BIND 9 branches (9.11, 9.11-S, 9.16, 9.16-S, 9.17) as well as all other versions of BIND 9.	7.5	More Details
CVE-2021-20092	The web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 do not properly restrict access to sensitive information from an unauthorized actor.	7.5	More Details
CVE-2020-7731	This affects all versions <0.7.0 of package github.com/russellhaering/gosaml2. There is a crash on nil-pointer dereference caused by sending malformed XML signatures.	7.5	More Details
CVE-2021-28899	Vulnerability in the AC3AudioFileServerMediaSubsession, ADTSAudioFileServerMediaSubsession, and AMRAudioFileServerMediaSubsessionLive OnDemandServerMediaSubsession subclasses in Networks LIVE555 Streaming Media before 2021.3.16.	7.5	More Details
CVE-2021-25811	MERCUSYS Mercury X18G 1.0.5 devices allow Denial of service via a crafted value to the POST listen_http_lan parameter. Upon subsequent device restarts after this vulnerability is exploted the device will not be able to access the webserver unless the listen_http_lan parameter to uhttpd.json is manually fixed.	7.5	More Details
CVE-2020-35756	An issue was discovered on Libre Wireless LS9 LS1.5/p7040 devices. There is a luci_service GETPASS Configuration Password Information Leak. The luci_service daemon running on port 7777 does not require authentication to return the device configuration password in cleartext when using the GETPASS command. As such, any unauthenticated person with access to port 7777 on the device will be able to leak the user's personal device configuration password by issuing the GETPASS command.	7.5	More Details
CVE-2020-22784	In Etherpad UeberDB < 0.4.4, due to MySQL omitting trailing spaces on char / varchar columns during comparisons, retrieving database records using UeberDB's MySQL connector could allow bypassing access controls enforced on key names.	7.5	More Details
CVE-2021-20228	A flaw was found in the Ansible Engine 2.9.18, where sensitive info is not masked by default and is not protected by the no_log feature when using the sub-option feature of the basic.py module. This flaw allows an attacker to obtain sensitive information. The highest threat from this vulnerability is to confidentiality.	7.5	More Details
CVE-2020-22782	Etherpad < 1.8.3 is affected by a denial of service in the import functionality. Upload of binary file to the import endpoint would crash the instance.	7.5	More Details
CVE-2021-3154	An issue was discovered in SolarWinds Serv-U before 15.2.2. Unauthenticated attackers can retrieve cleartext passwords via macro Injection. NOTE: this had a distinct fix relative to CVE-2020-35481.	7.5	More Details
CVE-2021-21535	Dell Hybrid Client versions prior to 1.5 contain a missing authentication for a critical function vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to gain root level access to the system.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1085	NVIDIA vGPU driver contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where there is the potential to write to a shared memory location and manipulate the data after the data has been validated, which may lead to denial of service and escalation of privileges and information disclosure but attacker doesn't have control over what information is obtained. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7).	7.3	More Details
CVE-2021-29242	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages.	7.3	More Details
CVE-2021-31933	A remote code execution vulnerability exists in Chamilo through 1.11.14 due to improper input sanitization of a parameter used for file uploads, and improper file-extension filtering for certain filenames (e.g., .phar or .pht). A remote authenticated administrator is able to upload a file containing arbitrary PHP code into specific directories via main/inc/lib/fileUpload.lib.php directory traversal to achieve PHP code execution.	7.2	More Details
CVE-2021-25152	A remote insecure deserialization vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	7.2	More Details
CVE-2021-21417	fluidsynth is a software synthesizer based on the SoundFont 2 specifications. A use after free violation was discovered in fluidsynth, that can be triggered when loading an invalid SoundFont file.	7.2	More Details
CVE-2021-30166	The NTP Server configuration function of the IP camera device is not verified with special parameters. Remote attackers can perform a command Injection attack and execute arbitrary commands after logging in with the privileged permission.	7.2	More Details
CVE-2021-29350	SQL injection in the getip function in conn/function.php in 发货100-设计素材下载系统 1.1 allows remote attackers to inject arbitrary SQL commands via the X-Forwarded-For header to admin/product_add.php.	7.2	More Details
CVE-2021-1086	NVIDIA vGPU driver contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where it allows guests to control unauthorized resources, which may lead to integrity and confidentiality loss or information disclosure. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7).	7.1	More Details
CVE-2021-29484	Ghost is a Node.js CMS. An unused endpoint added during the development of 4.0.0 has left sites vulnerable to untrusted users gaining access to Ghost Admin. Attackers can gain access by getting logged in users to click a link containing malicious code. Users do not need to enter credentials and may not know they've visited a malicious site. Ghost(Pro) has already been patched. We can find no evidence that the issue was exploited on Ghost(Pro) prior to the patch being added. Self-hosters are impacted if running Ghost a version between 4.0.0 and 4.3.2. Immediate action should be taken to secure your site. The issue has been fixed in 4.3.3, all 4.x sites should upgrade as soon as possible. As the endpoint is unused, the patch simply removes it. As a workaround blocking access to /ghost/preview can also mitigate the issue.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1476	A vulnerability in the CLI of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input for specific commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. To exploit this vulnerability, an attacker must have valid administrator-level credentials.	6.7	More Details
CVE-2021-20515	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366.	6.7	More Details
CVE-2021-1488	A vulnerability in the upgrade process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to inject commands that could be executed with root privileges on the underlying operating system (OS). This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by uploading a crafted upgrade package file to an affected device. A successful exploit could allow the attacker to inject commands that could be executed with root privileges on the underlying OS.	6.7	More Details
CVE-2020-20247	Mikrotik RouterOs before 6.46.5 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/traceroute process. An authenticated remote attacker can cause a Denial of Service due via the loop counter variable.	6.5	More Details
CVE-2020-20218	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/traceroute process. An authenticated remote attacker can cause a Denial of Service due via the loop counter variable.	6.5	More Details
CVE-2021-31926	AMP Application Deployment Service in CubeCoders AMP 2.1.x before 2.1.1.2 allows a remote, authenticated user to open ports in the local system firewall by crafting an HTTP(S) request directly to the applicable API endpoint (despite not having permission to make changes to the system's network configuration).	6.5	More Details
CVE-2020-28943	OX App Suite 7.10.4 and earlier allows SSRF via a snippet.	6.5	More Details
CVE-2021-20326	A user authorized to performing a specific type of find query may trigger a denial of service. This issue affects MongoDB Server v4.4 versions prior to 4.4.4.	6.5	More Details
CVE-2021-21229	Incorrect security UI in downloads in Google Chrome on Android prior to 90.0.4430.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	6.5	More Details
CVE-2021-1489	A vulnerability in filesystem usage management for Cisco Firepower Device Manager (FDM) Software could allow an authenticated, remote attacker to exhaust filesystem resources, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to the insufficient management of available filesystem resources. An attacker could exploit this vulnerability by uploading files to the device and exhausting available filesystem resources. A successful exploit could allow the attacker to cause database errors and cause the device to become unresponsive to web-based management. Manual intervention is required to free filesystem resources and return the device to an operational state.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26804	Insecure Permissions in Centreon Web versions 19.10.18, 20.04.8, and 20.10.2 allows remote attackers to bypass validation by changing any file extension to ".gif", then uploading it in the "Administration/ Parameters/ Images" section of the application.	6.5	More Details
CVE-2021-22330	There is an out of bounds write vulnerability in Huawei Smartphone HUAWEI P30 versions 9.1.0.131(C00E130R1P21) when processing a message. An unauthenticated attacker can exploit this vulnerability by sending specific message to the target device. Due to insufficient validation of the input parameter, successful exploit can cause the process and the service to be abnormal.	6.5	More Details
CVE-2021-31418	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4-47270. An attacker must first obtain the ability to execute low-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 initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12221.	6.5	More Details
CVE-2021-25164	A remote XML external entity vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	6.5	More Details
CVE-2020-22783	Etherpad <1.8.3 stored passwords used by users insecurely in the database and in log files. This affects every database backend supported by Etherpad.	6.5	More Details
CVE-2021-22327	There is an arbitrary memory write vulnerability in Huawei smart phone when processing file parsing. Due to insufficient validation of the input files, successful exploit could cause certain service abnormal. Affected product versions include:HUAWEI P30 versions 10.0.0.186(C10E7R5P1), 10.0.0.186(C461E4R3P1), 10.0.0.188(C00E85R2P11), 10.0.0.188(C01E88R2P11),10.0.0.188(C605E19R1P3), 10.0.0.190(C185E4R7P1), 10.0.0.190(C431E22R2P5), 10.0.0.190(C432E22R2P5),10.0.0.190(C605E19R1P3), 10.0.0.190(C636E4R3P4), 10.0.0.192(C635E3R2P4).	6.5	More Details
CVE-2021-21391	CKEditor 5 provides a WYSIWYG editing solution. This CVE affects the following npm packages: ckeditor5-engine, ckeditor5-font, ckeditor5-image, ckeditor5-list, ckeditor5-markdown-gfm, ckeditor5-media-embed, ckeditor5-paste-from-office, and ckeditor5-widget. Following an internal audit, a regular expression denial of service (ReDoS) vulnerability has been discovered in multiple CKEditor 5 packages. The vulnerability allowed to abuse particular regular expressions, which could cause a significant performance drop resulting in a browser tab freeze. It affects all users using the CKEditor 5 packages listed above at version <= 26.0.0. The problem has been recognized and patched. The fix will be available in version 27.0.0.	6.5	More Details
CVE-2021-25214	In BIND 9.8.5 -> 9.8.8, 9.9.3 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND 9 Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a malformed IXFR triggering the flaw described above, the named process will terminate due to a failed assertion the next time the transferred secondary zone is refreshed.	6.5	More Details
CVE-2021-29144	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29138	A remote disclosure of privileged information vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	6.5	More Details
CVE-2021-29141	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	6.5	More Details
CVE-2021-31417	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4-47270. An attacker must first obtain the ability to execute low-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 initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12131.	6.5	More Details
CVE-2021-31419	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4-47270. An attacker must first obtain the ability to execute low-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 initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12136.	6.5	More Details
CVE-2021-21547	Dell EMC Unity, UnityVSA, and Unity XT versions prior to 5.0.7.0.5.008 contain a plain-text password storage vulnerability when the Dell Upgrade Readiness Utility is run on the system. The credentials of the Unisphere Administrator are stored in plain text. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	6.4	More Details
CVE-2021-31779	The yoast_seo (aka Yoast SEO) extension before 7.2.1 for TYPO3 allows SSRF via a backend user account.	6.4	More Details
CVE-2021-22547	In IoT Devices SDK, there is an implementation of calloc() that doesn't have a length check. An attacker could pass in memory objects larger than the buffer and wrap around to have a smaller buffer than required, allowing the attacker access to the other parts of the heap. We recommend upgrading the Google Cloud IoT Device SDK for Embedded C used to 1.0.3 or greater.	6.3	More Details
CVE-2021-21536	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to register the client to a server in order to view sensitive information.	6.2	More Details
CVE-2021-21537	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to view and exfiltrate sensitive information on the system.	6.2	More Details
CVE-2021-29137	A remote URL redirection vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	6.1	More Details
CVE-2021-31935	OX App Suite 7.10.4 and earlier allows XSS via a crafted distribution list (payload in the common name) that is mishandled in the scheduling view.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23015	An open redirect issue was discovered in OPNsense through 20.1.5. The redirect parameter "url" in login page was not filtered and can redirect user to any website.	6.1	More Details
CVE-2021-31879	GNU Wget through 1.21.1 does not omit the Authorization header upon a redirect to a different origin, a related issue to CVE-2018-1000007.	6.1	More Details
CVE-2020-22789	Unauthenticated Stored XSS in FME Server versions 2019.2 and 2020.0 Beta allows a remote attacker to gain admin privileges by injecting arbitrary web script or HTML via the login page. The XSS is executed when an administrator accesses the logs.	6.1	More Details
CVE-2021-21541	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain a DOM-based cross-site scripting vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or JavaScript code to DOM environment in the browser. The malicious code is then executed by the web browser in the context of the vulnerable web application.	6.1	More Details
CVE-2021-28280	CSRF + Cross-site scripting (XSS) vulnerability in search.php in PHPFusion 9.03.110 allows remote attackers to inject arbitrary web script or HTML	6.1	More Details
CVE-2020-28945	OX App Suite 7.10.4 and earlier allows XSS via crafted content to reach an undocumented feature, such as ![](http://onerror=Function.constructor, in a Notes item.	6.1	More Details
CVE-2021-27933	pfSense 2.5.0 allows XSS via the services_wol_edit.php Description field.	6.1	More Details
CVE-2020-22808	An issue was found in yii2_fecshop 2.x. There is a reflected XSS vulnerability in the check cart page.	6.1	More Details
CVE-2021-31934	OX App Suite 7.10.4 and earlier allows XSS via a crafted contact object (payload in the position or company field) that is mishandled in the App Suite UI on a smartphone.	6.1	More Details
CVE-2021-28359	The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions <1.10.15 in 1.x series and affects 2.0.0 and 2.0.1 and 2.x series. This is the same as CVE-2020-13944 & CVE-2020-17515 but the implemented fix did not fix the issue completely. Update to Airflow 1.10.15 or 2.0.2. Please also update your Python version to the latest available PATCH releases of the installed MINOR versions, example update to Python 3.6.13 if you are on Python 3.6. (Those contain the fix for CVE-2021-23336 https://nvd.nist.gov/vuln/detail/CVE-2021-23336).	6.1	More Details
CVE-2020-1721	A flaw was found in the Key Recovery Authority (KRA) Agent Service in pki-core 10.10.5 where it did not properly sanitize the recovery ID during a key recovery request, enabling a reflected cross-site scripting (XSS) vulnerability. An attacker could trick an authenticated victim into executing specially crafted Javascript code.	6.1	More Details
CVE-2020-18022	Cross Site Scripting (XSS) in Qibosoft QiboCMS v7 and earlier allows remote attackers to execute arbitrary code or obtain sensitive information by injecting arbitrary commands in a HTTP request to the "ewebeditor\3.1.1\kindeditor.js" component.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25810	Cross site Scripting (XSS) vulnerability in MERCUSYS Mercury X18G 1.0.5 devices, via crafted values to the 'src_dport_start', 'src_dport_end', and 'dest_port' parameters.	6.1	More Details
CVE-2020-17999	Cross Site Scripting (XSS) in MiniCMS v1.10 allows remote attackers to execute arbitrary code by injecting commands via a crafted HTTP request to the component "/mc-admin/post-edit.php".	6.1	More Details
CVE-2021-30227	Cross Site Scripting (XSS) vulnerability in the article comments feature in emlog 6.0.	6.1	More Details
CVE-2020-18035	Cross Site Scripting (XSS) in Jeesns v1.4.2 allows remote attackers to execute arbitrary code by injecting commands into the "CKEditorFuncNum" parameter in the component "CkeditorUploadController.java".	6.1	More Details
CVE-2020-21993	In WEMS Limited Enterprise Manager 2.58, input passed to the GET parameter 'email' is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML code in a user's browser session in context of an affected site.	6.1	More Details
CVE-2021-29159	A cross-site scripting (XSS) vulnerability has been discovered in Nexus Repository Manager 3.x before 3.30.1. An attacker with a local account can create entities with crafted properties that, when viewed by an administrator, can execute arbitrary JavaScript in the context of the NXRM application.	6.1	More Details
CVE-2020-18084	Cross Site Scripting (XSS) in yzmCMS v5.2 allows remote attackers to execute arbitrary code by injecting commands into the "referer" field of a POST request to the component "/member/index/login.html" when logging in.	6.1	More Details
CVE-2021-2321	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-2021-1256	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite files on the file system of an affected device by using directory traversal techniques. A successful exploit could cause system instability if important system files are overwritten. This vulnerability is due to insufficient validation of user input for the file path in a specific CLI command. An attacker could exploit this vulnerability by logging in to a targeted device and issuing a specific CLI command with crafted user input. A successful exploit could allow the attacker to overwrite arbitrary files on the file system of the affected device. The attacker would need valid user credentials on the device.	6.0	More Details
CVE-2021-31421	This vulnerability allows local attackers to delete arbitrary files 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 delete arbitrary files in the context of the hypervisor. Was ZDI-CAN-12129.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31432	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. 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 IDE virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13190.	6.0	More Details
CVE-2021-31423	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. 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 initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12528.	6.0	More Details
CVE-2021-31431	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. 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 IDE virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13189.	6.0	More Details
CVE-2021-31430	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. 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 IDE virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13188.	6.0	More Details
CVE-2021-21539	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain a Time-of-check Time-of-use (TOCTOU) race condition vulnerability. A remote authenticated attacker could potentially exploit this vulnerability to gain elevated privileges when a user with higher privileges is simultaneously accessing iDRAC through the web interface.	5.9	More Details
CVE-2021-21540	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain a stack-based overflow vulnerability. A remote authenticated attacker could potentially exploit this vulnerability to overwrite configuration information by injecting arbitrarily large payload.	5.9	More Details
CVE-2021-1495	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of specific HTTP header parameters. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured file policy for HTTP packets and deliver a malicious payload.	5.8	More Details
CVE-2021-23383	The package handlebars before 4.7.7 are vulnerable to Prototype Pollution when selecting certain compiling options to compile templates coming from an untrusted source.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31427	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Open Tools Gate component. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13082.	5.6	More Details
CVE-2021-30027	md_analyze_line in md4c.c in md4c 0.4.7 allows attackers to trigger use of uninitialized memory, and cause a denial of service via a malformed Markdown document.	5.5	More Details
CVE-2021-3508	A flaw was found in PDFResurrect in version 0.22b. There is an infinite loop in get_xref_linear_skipped() in pdf.c via a crafted PDF file.	5.5	More Details
CVE-2021-30219	samurai 1.2 has a NULL pointer dereference in printstatus() function in build.c via a crafted build file.	5.5	More Details
CVE-2021-31231	The Alertmanager in Grafana Enterprise Metrics before 1.2.1 and Metrics Enterprise 1.2.1 has a local file disclosure vulnerability when experimental.alertmanager.enable-api is used. The HTTP basic auth password_file can be used as an attack vector to send any file content via a webhook. The alertmanager templates can be used as an attack vector to send any file content because the alertmanager can load any text file specified in the templates list.	5.5	More Details
CVE-2021-31232	The Alertmanager in CNCF Cortex before 1.8.1 has a local file disclosure vulnerability when -experimental.alertmanager.enable-api is used. The HTTP basic auth password_file can be used as an attack vector to send any file content via a webhook. The alertmanager templates can be used as an attack vector to send any file content because the alertmanager can load any text file specified in the templates list.	5.5	More Details
CVE-2021-30218	samurai 1.2 has a NULL pointer dereference in writefile() in util.c via a crafted build file.	5.5	More Details
CVE-2021-1087	NVIDIA vGPU driver contains a vulnerability in the Virtual GPU Manager (vGPU plugin), which could allow an attacker to retrieve information that could lead to a Address Space Layout Randomization (ASLR) bypass. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7).	5.5	More Details
CVE-2021-31778	The media2click (aka 2 Clicks for External Media) extension 1.x before 1.3.3 for TYPO3 allows XSS by a backend user account.	5.4	More Details
CVE-2020-4987	The IBM FlashSystem 900 user management GUI is vulnerable to stored cross-site scripting in code versions 1.5.2.8 and prior and 1.6.1.2 and prior. 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.	5.4	More Details
CVE-2021-29387	Multiple stored cross-site scripting (XSS) vulnerabilities in Sourcecodester Equipment Inventory System 1.0 allow remote attackers to inject arbitrary javascript via any "Add" sections, such as Add Item , Employee and Position or others in the Name Parameters.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1369	A vulnerability in the REST API of Cisco Firepower Device Manager (FDM) On-Box Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected device. This vulnerability is due to the improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by sending malicious requests that contain references in XML entities to an affected system. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information or causing a partial denial of service (DoS) condition on the affected device.	5.4	More Details
CVE-2021-29388	A stored cross-site scripting (XSS) vulnerability in SourceCodester Budget Management System 1.0 allows users to inject and store arbitrary JavaScript code in index.php via vulnerable field 'Budget Title'.	5.4	More Details
CVE-2021-31792	XSS in the client account page in SuiteCRM before 7.11.19 allows an attacker to inject JavaScript via the name field	5.4	More Details
CVE-2021-29146	A remote cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	5.4	More Details
CVE-2020-22790	Authenticated Stored XSS in FME Server versions 2019.2 and 2020.0 Beta allows a remote attacker to execute codeby injecting arbitrary web script or HTML via modifying the name of the users. The XSS is executed when an administrator access the logs.	5.4	More Details
CVE-2020-21101	Cross Site Scriptiong vulnerabilityin Screenly screenly-ose all versions, including v1.8.2 (2019-09-25-Screenly-OSE-lite.img), in the 'Add Asset' page via manipulation of a 'URL' field, which could let a remote malicious user execute arbitrary code.	5.4	More Details
CVE-2021-30169	The sensitive information of webcam device is not properly protected. Remote attackers can unauthentically grant user’s credential.	5.3	More Details
CVE-2021-30048	Directory Traversal in the fileDownload function in com/java2nb/common/controller/FileController.java in Novel-plus (小说精品屋-plus) 3.5.1 allows attackers to read arbitrary files via the filePath parameter.	5.3	More Details
CVE-2021-31865	Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows users to circumvent the allowed filename extensions of uploaded attachments.	5.3	More Details
CVE-2021-31866	Redmine before 4.0.9 and 4.1.x before 4.1.3 allows an attacker to learn the values of internal authentication keys by observing timing differences in string comparison operations within SysController and MailHandlerController.	5.3	More Details
CVE-2021-23364	The package browserslist from 4.0.0 and before 4.16.5 are vulnerable to Regular Expression Denial of Service (ReDoS) during parsing of queries.	5.3	More Details
CVE-2021-31864	Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows attackers to bypass the add_issue_notes permission requirement by leveraging the incoming mail handler.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23343	All versions of package path-parse are vulnerable to Regular Expression Denial of Service (ReDoS) via splitDeviceRe, splitTailRe, and splitPathRe regular expressions. ReDoS exhibits polynomial worst-case time complexity.	5.3	More Details
CVE-2021-21264	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. A bypass of CVE-2020-26231 (fixed in 1.0.470/471 and 1.1.1) was discovered that has the same impact as CVE-2020-26231 & CVE-2020-15247. An authenticated backend user with the `cms.manage_pages`, `cms.manage_layouts`, or `cms.manage_partials` permissions who would **normally** not be permitted to provide PHP code to be executed by the CMS due to `cms.enableSafeMode` being enabled is able to write specific Twig code to escape the Twig sandbox and execute arbitrary PHP. This is not a problem for anyone that trusts their users with those permissions to normally write & manage PHP within the CMS by not having `cms.enableSafeMode` enabled, but would be a problem for anyone relying on `cms.enableSafeMode` to ensure that users with those permissions in production do not have access to write & execute arbitrary PHP. Issue has been patched in Build 472 (v1.0.472) and v1.1.2. As a workaround, apply https://github.com/octobercms/october/commit/f63519ff1e8d375df30deba63156a2fc97aa9ee7 to your installation manually if unable to upgrade to Build 472 or v1.1.2.	5.2	More Details
CVE-2021-20266	A flaw was found in RPM's hdrblobInit() in lib/header.c. This flaw allows an attacker who can modify the rpmdb to cause an out-of-bounds read. The highest threat from this vulnerability is to system availability.	4.9	More Details
CVE-2021-31777	The dce (aka Dynamic Content Element) extension 2.2.0 through 2.6.x before 2.6.2, and 2.7.x before 2.7.1, for TYPO3 allows SQL Injection via a backend user account.	4.9	More Details
CVE-2021-1458	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-29139	A remote cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	4.8	More Details
CVE-2021-29142	A remote cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	4.8	More Details
CVE-2021-21542	Dell EMC iDRAC9 versions prior to 4.40.10.00 contain multiple stored cross-site scripting vulnerabilities. A remote authenticated malicious user with high privileges could potentially exploit these vulnerabilities to store malicious HTML or JavaScript code through multiple affected while generating a certificate. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1457	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-1456	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-1455	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-21543	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain multiple stored cross-site scripting vulnerabilities. A remote authenticated malicious user with high privileges could potentially exploit these vulnerabilities to store malicious HTML or JavaScript code through multiple affected parameters. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	4.8	More Details
CVE-2021-3511	Disclosure of sensitive information to an unauthorized user vulnerability in Buffalo broadband routers (BHR-4GRV firmware Ver.1.99 and prior, DWR-HP-G300NH firmware Ver.1.83 and prior, HW-450HP-ZWE firmware Ver.1.99 and prior, WHR-300HP firmware Ver.1.99 and prior, WHR-300 firmware Ver.1.99 and prior, WHR-G301N firmware Ver.1.86 and prior, WHR-HP-G300N firmware Ver.1.99 and prior, WHR-HP-GN firmware Ver.1.86 and prior, WPL-05G300 firmware Ver.1.87 and prior, WZR-450HP-CWT firmware Ver.1.99 and prior, WZR-450HP-UB firmware Ver.1.99 and prior, WZR-HP-AG300H firmware Ver.1.75 and prior, WZR-HP-G300NH firmware Ver.1.83 and prior, WZR-HP-G301NH firmware Ver.1.83 and prior, WZR-HP-G302H firmware Ver.1.85 and prior, WZR-HP-G450H firmware Ver.1.89 and prior, WZR-300HP firmware Ver.1.99 and prior, WZR-450HP firmware Ver.1.99 and prior, WZR-600DHP firmware Ver.1.99 and prior, WZR-D1100H firmware Ver.1.99 and prior, FS-HP-G300N firmware Ver.3.32 and prior, FS-600DHP firmware Ver.3.38 and prior, FS-R600DHP firmware Ver.3.39 and prior, and FS-G300N firmware Ver.3.13 and prior) allows remote unauthenticated attackers to obtain information such as configuration via unspecified vectors.	4.3	More Details
CVE-2021-21228	Insufficient policy enforcement in extensions in Google Chrome prior to 90.0.4430.93 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1477	A vulnerability in an access control mechanism of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to access services beyond the scope of their authorization. This vulnerability is due to insufficient enforcement of access control in the affected software. An attacker could exploit this vulnerability by directly accessing the internal services of an affected device. A successful exploit could allow the attacker to overwrite policies and impact the configuration and operation of the affected device.	4.3	More Details
CVE-2021-21534	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to gain access to sensitive information via the local API.	4.0	More Details
CVE-2021-29463	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.	3.3	More Details
CVE-2021-29464	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A heap buffer overflow was found in Exiv2 versions v0.27.3 and earlier. The heap overflow is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, 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.	3.3	More Details
CVE-2021-31815	GAEN (aka Google/Apple Exposure Notifications) through 2021-04-27 on Android allows attackers to obtain sensitive information, such as a user's location history, in-person social graph, and (sometimes) COVID-19 infection status, because Rolling Proximity Identifiers and MAC addresses are written to the Android system log, and many Android devices have applications (preinstalled by the hardware manufacturer or network operator) that read system log data and send it to third parties. NOTE: a news outlet (The Markup) states that they received a vendor response indicating that fix deployment "began several weeks ago and will be complete in the coming days."	3.3	More Details
CVE-2021-21544	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain an improper authentication vulnerability. A remote authenticated malicious user with high privileges could potentially exploit this vulnerability to manipulate the username field under the comment section and set the value to any user.	2.7	More Details
CVE-2021-20095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-27802	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-24177. Reason: This candidate is a duplicate of CVE-2021-24177. Notes: All CVE users should reference CVE-2021-24177 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details