SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 July 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-2021-25320	A Improper Access Control vulnerability in Rancher, allows users in the cluster to make request to cloud providers by creating requests with the cloud-credential ID. Rancher in this case would attach the requested credentials without further checks This issue affects: Rancher versions prior to 2.5.9; Rancher versions prior to 2.4.16.	9.9	More Details
CVE-2021-34458	Windows Kernel Remote Code Execution Vulnerability	9.9	More Details
CVE-2021-25953	Prototype pollution vulnerability in 'putil-merge' versions1.0.0 through 3.6.6 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0515	In Factory::CreateStrictFunctionMap of factory.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-167389063	9.8	More Details
CVE-2020-5349	Dell EMC Networking S4100 and S5200 Series Switches manufactured prior to February 2020 contain a hardcoded credential vulnerability. A remote unauthenticated malicious user could exploit this vulnerability and gain administrative privileges.	9.8	More Details
CVE-2021-20110	Due to Manage Engine Asset Explorer Agent 1.0.34 not validating HTTPS certificates, an attacker on the network can statically configure their IP address to match the Asset Explorer's Server IP address. This will allow an attacker to send a NEWSCAN request to a listening agent on the network as well as receive the agent's HTTP request verifying its authtoken. In httphandler.cpp, the agent reaching out over HTTP is vulnerable to an Integer Overflow, which can be turned into a Heap Overflow allowing for remote code execution as NT AUTHORITY/SYSTEM on the agent machine. The Integer Overflow occurs when receiving POST response from the Manage Engine server, and the agent calling "HttpQueryInfoW" in order to get the "Content-Length" size from the incoming POST request. This size is taken, but multiplied to a larger amount. If an attacker specifies a Content-Length size of 1073741823 or larger, this integer arithmetic will wrap the value back around to smaller integer, then calls "calloc" with this size to allocate memory. The following API "InternetReadFile" will copy the POST data into this buffer, which will be too small for the contents, and cause heap overflow.	9.8	More Details
CVE-2021-35965	The Orca HCM digital learning platform uses a weak factory default administrator password, which is hard-coded in the source code of the webpage in plain text, thus remote attackers can obtain administrator’s privilege without logging in.	9.8	More Details
CVE-2021-35963	The specific parameter of upload function of the Orca HCM digital learning platform does not filter file format, which allows remote unauthenticated attackers to upload files containing malicious script to execute RCE attacks.	9.8	More Details
CVE-2021-33027	Sylabs Singularity Enterprise through 1.6.2 has Insufficient Entropy in a nonce.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33592	NAVER Toolbar before 4.0.30.323 allows remote attackers to execute arbitrary code via a crafted upgrade.xml file. Special characters in filename parameter can be the cause of bypassing code signing check function.	9.8	More Details
CVE-2021-33911	Zoho ManageEngine ADManager Plus before 7110 allows remote code execution.	9.8	More Details
CVE-2020-4821	IBM InfoSphere Data Replication 11.4 and IBM InfoSphere Change Data Capture for z/OS 10.2.1, under certain configurations, could allow a user to bypass authentication mechanisms using an empty password string. IBM X-Force ID: 189834	9.8	More Details
CVE-2021-35961	Dr. ID Door Access Control and Personnel Attendance Management system uses the hard-code admin default credentials that allows remote attackers to access the system through the default password and obtain the highest permission.	9.8	More Details
CVE-2021-21820	A hard-coded password vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to code execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.8	More Details
CVE-2021-21804	A local file inclusion (LFI) vulnerability exists in the options.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). A specially crafted HTTP request can lead to arbitrary PHP code execution. An attacker can send a crafted HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-0276	A stack-based Buffer Overflow vulnerability in Juniper Networks SBR Carrier with EAP (Extensible Authentication Protocol) authentication configured, allows an attacker sending specific packets causing the radius daemon to crash resulting with a Denial of Service (DoS) or leading to remote code execution (RCE). By continuously sending this specific packets, an attacker can repeatedly crash the radius daemon, causing a sustained Denial of Service (DoS). This issue affects Juniper Networks SBR Carrier: 8.4.1 versions prior to 8.4.1R19; 8.5.0 versions prior to 8.5.0R10; 8.6.0 versions prior to 8.6.0R4.	9.8	More Details
CVE-2020-11633	The Zscaler Client Connector for Windows prior to 2.1.2.74 had a stack based buffer overflow when connecting to misconfigured TLS servers. An adversary would potentially have been able to execute arbitrary code with system privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34690	iDrive RemotePC before 7.6.48 on Windows allows authentication bypass. A remote and unauthenticated attacker can bypass cloud authentication to connect and control a system via TCP port 5970 and 5980.	9.8	More Details
CVE-2020-24133	A heap buffer overflow vulnerability in the r_asm_swf_disass function of Radare2-extras before commit e74a93c allows attackers to execute arbitrary code or carry out denial of service (DOS) attacks.	9.8	More Details
CVE-2020-18155	SQL Injection vulnerability in Subrion CMS v4.2.1 in the search page if a website uses a PDO connection.	9.8	More Details
CVE-2020-18144	SQL Injection Vulnerability in ECTouch v2 via the integral_min parameter in index.php.	9.8	More Details
CVE-2020-35427	SQL injection vulnerability in PHPGurukul Employee Record Management System 1.1 allows remote attackers to execute arbitrary SQL commands and bypass authentication.	9.8	More Details
CVE-2021-33501	Overwolf Client 0.169.0.22 allows XSS, with resultant Remote Code Execution, via an overwolfstore:// URL.	9.6	More Details
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	9.1	More Details
CVE-2020-5322	Dell EMC OpenManage Enterprise-Modular (OME-M) versions prior to 1.10.00 contain a command injection vulnerability. A remote authenticated malicious user with high privileges could potentially exploit the vulnerability to execute arbitrary shell commands on the affected system.	9.1	More Details
CVE-2021-22779	Authentication Bypass by Spoofing vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Control Expert V15.0 SP1, EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), SCADAPack RemoteConnect for x70 (all versions), Modicon M580 CPU (all versions - part numbers BMEP* and BMEH*), Modicon M340 CPU (all versions - part numbers BMXP34*), that could cause unauthorized access in read and write mode to the controller by spoofing the Modbus communication between the engineering software and the controller.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35211	Microsoft discovered a remote code execution (RCE) vulnerability in the SolarWinds Serv-U product utilizing a Remote Memory Escape Vulnerability. If exploited, a threat actor may be able to gain privileged access to the machine hosting Serv-U Only. SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP for Windows before 15.2.3 HF2 are affected by this vulnerability.	9.0	More Details
CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability	9.0	More Details
CVE-2020-5320	Dell EMC OpenManage Enterprise (OME) versions prior to 3.2 and OpenManage Enterprise-Modular (OME-M) versions prior to 1.10.00 contain a SQL injection vulnerability. A remote authenticated malicious user with high privileges could potentially exploit this vulnerability to execute SQL commands to perform unauthorized actions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-0277	An Out-of-bounds Read vulnerability in the processing of specially crafted LLDP frames by the Layer 2 Control Protocol Daemon (l2cpd) of Juniper Networks Junos OS and Junos OS Evolved may allow an attacker to cause a Denial of Service (DoS), or may lead to remote code execution (RCE). Continued receipt and processing of these frames, sent from the local broadcast domain, will repeatedly crash the l2cpd process and sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S18; 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved versions prior to 20.4R2-EVO.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34828	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the SOAPAction HTTP header. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-12066.	8.8	More Details
CVE-2021-34829	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the HNAP_AUTH HTTP header. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-12065.	8.8	More Details
CVE-2021-0278	An Improper Input Validation vulnerability in J-Web of Juniper Networks Junos OS allows a locally authenticated attacker to escalate their privileges to root over the target device. junos:18.3R3-S5 junos:18.4R3-S9 junos:19.1R3-S6 junos:19.3R2-S6 junos:19.3R3-S3 junos:19.4R1-S4 junos:19.4R3-S4 junos:20.1R2-S2 junos:20.1R3 junos:20.2R3-S1 junos:20.3X75-D20 junos:20.3X75-D30 junos:20.4R2-S1 junos:20.4R3 junos:21.1R1-S1 junos:21.1R2 junos:21.2R1 junos:21.3R1 This issue affects: Juniper Networks Junos OS 19.3 versions 19.3R1 and above prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	8.8	More Details
CVE-2021-31590	PwnDoc all versions until 0.4.0 (2021-08-23) has incorrect JSON Webtoken handling, leading to incorrect access control. With a valid JSON Webtoken that is used for authentication and authorization, a user can keep his admin privileges even if he is downgraded to the "user" privilege. Even after a user's account is deleted, the user can still access the administration panel (and add or delete users) and has complete access to the system.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34830	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the Cookie HTTP header. 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 device. Was ZDI-CAN-12028.	8.8	More Details
CVE-2021-31999	A Reliance on Untrusted Inputs in a Security Decision vulnerability in Rancher allows users in the cluster to act as others users in the cluster by forging the "Impersonate-User" or "Impersonate-Group" headers. This issue affects: Rancher versions prior to 2.5.9. Rancher versions prior to 2.4.16.	8.8	More Details
CVE-2021-36799	KNX ETS5 through 5.7.6 uses the hard-coded password ETS5Password, with a salt value of Ivan Medvedev, allowing local users to read project information. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2021-25318	A Incorrect Permission Assignment for Critical Resource vulnerability in Rancher allows users in the cluster to modify resources they should not have access to. This issue affects: Rancher versions prior to 2.5.9 ; Rancher versions prior to 2.4.16.	8.8	More Details
CVE-2021-34508	Windows Kernel Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-32739	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. From version 2.4.0 through version 2.12.4, a vulnerability exists that may allow privilege escalation for authenticated API users. With a read-ony user's credentials, an attacker can view most attributes of all config objects including `ticket_salt` of `ApiListener`. This salt is enough to compute a ticket for every possible common name (CN). A ticket, the master node's certificate, and a self-signed certificate are enough to successfully request the desired certificate from Icinga. That certificate may in turn be used to steal an endpoint or API user's identity. Versions 2.12.5 and 2.11.10 both contain a fix the vulnerability. As a workaround, one may either specify queryable types explicitly or filter out ApiListener objects.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34442	Windows DNS Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-34481	A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. UPDATE August 10, 2021: Microsoft has completed the investigation and has released security updates to address this vulnerability. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. This security update changes the Point and Print default behavior; please see KB5005652.	8.8	More Details
CVE-2021-33780	Windows DNS Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-34525	Windows DNS Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-0592	In various functions in WideVine, there are possible out of bounds writes due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-188061006	8.8	More Details
CVE-2021-24453	The Include Me WordPress plugin through 1.2.1 is vulnerable to path traversal / local file inclusion, which can lead to Remote Code Execution (RCE) of the system due to log poisoning and therefore potentially a full compromise of the underlying structure	8.8	More Details
CVE-2021-34494	Windows DNS Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-5315	Dell EMC Repository Manager (DRM) version 3.2 contains a plain-text password storage vulnerability. Proxy server user password is stored in a plain text in a local database. A local authenticated malicious user with access to the local file system may use the exposed password to access the with privileges of the compromised user.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36428	matio (aka MAT File I/O Library) 1.5.18 through 1.5.21 has a heap-based buffer overflow in ReadInt32DataDouble (called from ReadInt32Data and Mat_VarRead4).	8.8	More Details
CVE-2020-15660	Missing checks on Content-Type headers in geckodriver before 0.27.0 could lead to a CSRF vulnerability, that might, when paired with a specifically prepared request, lead to remote code execution.	8.8	More Details
CVE-2021-20781	Cross-site request forgery (CSRF) vulnerability in WordPress Meta Data Filter & Taxonomies Filter versions prior to v.1.2.8 and versions prior to v.2.2.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2021-20782	Cross-site request forgery (CSRF) vulnerability in Software License Manager versions prior to 4.4.6 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2021-36230	HashiCorp Terraform Enterprise releases up to v202106-1 did not properly perform authorization checks on a subset of API requests executed using the run token, allowing privilege escalation to organization owner. Fixed in v202107-1.	8.8	More Details
CVE-2021-33752	Windows DNS Snap-in Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28053	An issue was discovered in Centreon-Web in Centreon Platform 20.10.0. A SQL injection vulnerability in "Configuration > Users > Contacts / Users" allows remote authenticated users to execute arbitrary SQL commands via the Additional Information parameters.	8.8	More Details
CVE-2021-34827	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the SOAPAction HTTP header. 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 device. Was ZDI-CAN-12029.	8.8	More Details
CVE-2021-33750	Windows DNS Snap-in Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3246	A heap buffer overflow vulnerability in msadpcm_decode_block of libsndfile 1.0.30 allows attackers to execute arbitrary code via a crafted WAV file.	8.8	More Details
CVE-2021-33671	SAP NetWeaver Guided Procedures (Administration Workset), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. The impact of missing authorization could result to abuse of functionality restricted to a particular user group, and could allow unauthorized users to read, modify or delete restricted data.	8.8	More Details
CVE-2021-33749	Windows DNS Snap-in Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-27021	A flaw was discovered in Puppet DB, this flaw results in an escalation of privileges which allows the user to delete tables via an SQL query.	8.8	More Details
CVE-2021-33756	Windows DNS Snap-in Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-7866	When using XPLATFORM 9.2.2.270 or earlier versions ActiveX component, arbitrary commands can be executed due to improper input validation	8.8	More Details
CVE-2021-32743	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. In versions prior to 2.11.10 and from version 2.12.0 through version 2.12.4, some of the Icinga 2 features that require credentials for external services expose those credentials through the API to authenticated API users with read permissions for the corresponding object types. IdoMysqlConnection and IdoPgsqlConnection (every released version) exposes the password of the user used to connect to the database. IcingaDB (added in 2.12.0) exposes the password used to connect to the Redis server. ElasticsearchWriter (added in 2.8.0)exposes the password used to connect to the Elasticsearch server. An attacker who obtains these credentials can impersonate Icinga to these services and add, modify and delete information there. If credentials with more permissions are in use, this increases the impact accordingly. Starting with the 2.11.10 and 2.12.5 releases, these passwords are no longer exposed via the API. As a workaround, API user permissions can be restricted to not allow querying of any affected objects, either by explicitly listing only the required object types for object query permissions, or by applying a filter rule.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0279	Juniper Networks Contrail Cloud (CC) releases prior to 13.6.0 have RabbitMQ service enabled by default with hardcoded credentials. The messaging services of RabbitMQ are used when coordinating operations and status information among Contrail services. An attacker with access to an administrative service for RabbitMQ (e.g. GUI), can use these hardcoded credentials to cause a Denial of Service (DoS) or have access to unspecified sensitive system information. This issue affects the Juniper Networks Contrail Cloud releases on versions prior to 13.6.0.	8.6	More Details
CVE-2021-34450	Windows Hyper-V Remote Code Execution Vulnerability	8.5	More Details
CVE-2021-33767	Open Enclave SDK Elevation of Privilege Vulnerability	8.2	More Details
CVE-2019-3752	Dell EMC Avamar Server versions 7.4.1, 7.5.0, 7.5.1, 18.2 and 19.1 and Dell EMC Integrated Data Protection Appliance (IDPA) versions 2.0, 2.1, 2.2, 2.3 and 2.4. contain an XML External Entity(XXE) Injection vulnerability. A remote unauthenticated malicious user could potentially exploit this vulnerability to cause Denial of Service or information exposure by supplying specially crafted document type definitions (DTDs) in an XML request.	8.2	More Details
CVE-2021-34469	Microsoft Office Security Feature Bypass Vulnerability	8.2	More Details
CVE-2021-33779	Windows AD FS Security Feature Bypass Vulnerability	8.1	More Details
CVE-2021-21586	Wyse Management Suite versions 3.2 and earlier contain an absolute path traversal vulnerability. A remote authenticated malicious user could exploit this vulnerability in order to read arbitrary files on the system.	8.1	More Details
CVE-2021-33781	Azure AD Security Feature Bypass Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32764	Discourse is an open-source discussion platform. In Discourse versions 2.7.5 and prior, parsing and rendering of YouTube Oneboxes can be susceptible to XSS attacks. This vulnerability only affects sites which have modified or disabled Discourse's default Content Security Policy. The issue is patched in `stable` version 2.7.6, `beta` version 2.8.0.beta3, and `tests-passed` version 2.8.0.beta3. As a workaround, ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.	8.1	More Details
CVE-2021-31216	Siren Investigate before 11.1.1 contains a server side request forgery (SSRF) defect in the built-in image proxy route (which is enabled by default). An attacker with access to the Investigate installation can specify an arbitrary URL in the parameters of the image proxy route and fetch external URLs as the Investigate process on the host.	8.1	More Details
CVE-2021-34520	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-0514	In several functions of the V8 library, there is a possible use after free due to a race condition. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9 Android-11 Android-8.1Android ID: A-162604069	8.1	More Details
CVE-2021-33786	Windows LSA Security Feature Bypass Vulnerability	8.1	More Details
CVE-2021-34492	Windows Certificate Spoofing Vulnerability	8.1	More Details
CVE-2020-12734	DEPSTECH WiFi Digital Microscope 3 allows remote attackers to change the SSID and password, and demand a ransom payment from the rightful device owner, because there is no way to reset to Factory Default settings.	8.1	More Details
CVE-2021-34474	Dynamics Business Central Remote Code Execution Vulnerability	8.0	More Details
CVE-2021-33768	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34446	Windows HTML Platforms Security Feature Bypass Vulnerability	8.0	More Details
CVE-2021-33746	Windows DNS Server Remote Code Execution Vulnerability	8.0	More Details
CVE-2021-29742	IBM Security Verify Access Docker 10.0.0 could allow a user to impersonate another user on the system. IBM X-Force ID: 201483.	8.0	More Details
CVE-2021-34470	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.0	More Details
CVE-2021-0594	In onCreate of ConfirmConnectActivity, there is a possible remote bypass of user consent due to improper input validation. This could lead to remote (proximal, NFC) escalation of privilege allowing an attacker to deceive a user into allowing a Bluetooth connection with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176445224	8.0	More Details
CVE-2021-33754	Windows DNS Server Remote Code Execution Vulnerability	8.0	More Details
CVE-2021-34501	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34510	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34516	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34498	Windows GDI Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-33759	Windows Desktop Bridge Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34518	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-33761	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36753	sharkdp BAT before 0.18.2 executes less.exe from the current working directory.	7.8	More Details
CVE-2021-34503	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34504	Windows Address Book Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34511	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-33784	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-33771	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34489	DirectWrite Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34488	Windows Console Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34479	Microsoft Visual Studio Spoofing Vulnerability	7.8	More Details
CVE-2021-34514	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33773	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34513	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-33775	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-33776	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-33777	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-33778	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34477	Visual Studio Code .NET Runtime Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-11632	The Zscaler Client Connector prior to 2.1.2.150 did not quote the search path for services, which allows a local adversary to execute code with system privileges.	7.8	More Details
CVE-2021-34512	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-11634	The Zscaler Client Connector for Windows prior to 2.1.2.105 had a DLL hijacking vulnerability caused due to the configuration of OpenSSL. A local adversary may be able to execute arbitrary code in the SYSTEM context.	7.8	More Details
CVE-2021-34692	iDrive RemotePC before 7.6.48 on Windows allows privilege escalation. A local and low-privileged user can force RemotePC to execute an attacker-controlled executable with SYSTEM privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34439	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0602	In onCreateOptionsMenu of WifiNetworkDetailsFragment.java, there is a possible way for guest users to view and modify Wi-Fi settings for all configured APs due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-177573895	7.8	More Details
CVE-2021-34529	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34521	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0600	In onCreate of DeviceAdminAdd.java, there is a possible way to mislead a user to activate a device admin app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-179042963	7.8	More Details
CVE-2021-35449	The Lexmark Universal Print Driver version 2.15.1.0 and below, G2 driver 2.7.1.0 and below, G3 driver 3.2.0.0 and below, and G4 driver 4.2.1.0 and below are affected by a privilege escalation vulnerability. A standard low priviliged user can use the driver to execute a DLL of their choosing during the add printer process, resulting in escalation of privileges to SYSTEM.	7.8	More Details
CVE-2021-29707	IBM HMC (Hardware Management Console) V9.1.910.0 and V9.2.950.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 200879.	7.8	More Details
CVE-2021-0589	In BTM_TryAllocateSCN of btm_scn.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180939982	7.8	More Details
CVE-2020-29157	An issue in RAONWIZ K Editor v2018.0.0.10 allows attackers to perform a DLL hijacking attack when the service or system is restarted.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0587	In StreamOut::prepareForWriting of StreamOut.cpp, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185259758	7.8	More Details
CVE-2021-0586	In onCreate of DevicePickerFragment.java, there is a possible way to trick the user to select an unwanted bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-182584940	7.8	More Details
CVE-2021-0577	In flv extractor, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187161771	7.8	More Details
CVE-2021-0486	In onPackageAddedInternal of PermissionManagerService.java, there is possible access to external storage due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-171430330	7.8	More Details
CVE-2020-0417	In setNiNotification of GpsNetInitiatedHandler.java, there is a possible permissions bypass due to an empty mutable PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-154319182	7.8	More Details
CVE-2021-33505	A local malicious user can circumvent the Falco detection engine through 0.28.1 by running a program that alters arguments of system calls being executed. Issue is fixed in Falco versions >= 0.29.1.	7.8	More Details
CVE-2021-35469	The Lexmark Printer Software G2, G3 and G4 Installation Packages have a local escalation of privilege vulnerability due to a registry entry that has an unquoted service path.	7.8	More Details
CVE-2019-25050	netCDF in GDAL 2.4.2 through 3.0.4 has a stack-based buffer overflow in nc4_get_att (called from nc4_get_att_tc and nc_get_att_text) and in uffd_cleanup (called from netCDFDataset::~netCDFDataset and netCDFDataset::~netCDFDataset).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25051	objstack in GNU Aspell 0.60.8 has a heap-based buffer overflow in acommon::ObjStack::dup_top (called from acommon::StringMap::add and acommon::Config::lookup_list).	7.8	More Details
CVE-2020-36430	libass 0.15.x before 0.15.1 has a heap-based buffer overflow in decode_chars (called from decode_font and process_text) because the wrong integer data type is used for subtraction.	7.8	More Details
CVE-2020-15496	Acronis True Image for Mac before 2021 Update 4 allowed local privilege escalation due to insecure folder permissions.	7.8	More Details
CVE-2020-25736	Acronis True Image 2019 update 1 through 2021 update 1 on macOS allows local privilege escalation due to an insecure XPC service configuration.	7.8	More Details
CVE-2021-32463	An incorrect permission assignment denial-of-service vulnerability in Trend Micro Apex One, Apex One as a Service (SaaS), Worry-Free Business Security 10.0 SP1 and Worry-Free Servgices could allow a local attacker to escalate privileges and delete files with system privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2020-15495	Acronis True Image 2019 update 1 through 2020 on macOS allows local privilege escalation due to an insecure XPC service configuration.	7.8	More Details
CVE-2021-33909	fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05.	7.8	More Details
CVE-2021-0603	In onCreate of ContactSelectionActivity.java, there is a possible way to get access to contacts without permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-182809425	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3042	A local privilege escalation (PE) vulnerability exists in the Palo Alto Networks Cortex XDR agent on Windows platforms that enables an authenticated local Windows user to execute programs with SYSTEM privileges. Exploiting this vulnerability requires the user to have file creation privilege in the Windows root directory (such as C:\). This issue impacts: All versions of Cortex XDR agent 6.1 without content update 181 or a later version; All versions of Cortex XDR agent 7.2 without content update 181 or a later version; All versions of Cortex XDR agent 7.3 without content update 181 or a later version. Cortex XDR agent 5.0 versions are not impacted by this issue. Content updates are required to resolve this issue and are automatically applied for the agent.	7.8	More Details
CVE-2021-34528	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34452	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-34522	Microsoft Defender Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-33743	Windows Projected File System Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-33740	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31979	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34438	Windows Font Driver Host Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31947	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34441	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-3550	A DLL search path vulnerability was reported in Lenovo PCManager, prior to version 3.0.500.5102, that could allow privilege escalation.	7.8	More Details
CVE-2021-31859	Incorrect privileges in the MU55 FlexiSpooler service in YSoft SafeQ 6 6.0.55 allows local user privilege escalation by overwriting the executable file via an alternative data stream.	7.8	More Details
CVE-2021-34445	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34455	Windows File History Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34456	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34459	Windows AppContainer Elevation Of Privilege Vulnerability	7.8	More Details
CVE-2021-34460	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34461	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34464	Microsoft Defender Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-25445	The “Subscribe” feature in Ultimate Booking System Booking Core 1.7.0 is vulnerable to CSV formula injection. The input containing the excel formula is not being sanitized by the application. As a result when admin in backend download and open the csv, content of the cells are executed.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33758	Windows Hyper-V Denial of Service Vulnerability	7.7	More Details
CVE-2021-1422	A vulnerability in the software cryptography module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker or an unauthenticated attacker in a man-in-the-middle position to cause an unexpected reload of the device that results in a denial of service (DoS) condition. The vulnerability is due to a logic error in how the software cryptography module handles specific types of decryption errors. An attacker could exploit this vulnerability by sending malicious packets over an established IPsec connection. A successful exploit could cause the device to crash, forcing it to reload. Important: Successful exploitation of this vulnerability would not cause a compromise of any encrypted data. Note: This vulnerability affects only Cisco ASA Software Release 9.16.1 and Cisco FTD Software Release 7.0.0.	7.7	More Details
CVE-2021-31206	Microsoft Exchange Server Remote Code Execution Vulnerability	7.6	More Details
CVE-2020-5321	Dell EMC OpenManage Enterprise (OME) versions prior to 3.2 and OpenManage Enterprise-Modular (OME-M) versions prior to 1.10.00 contain an improper input validation vulnerability. A remote authenticated malicious user with high privileges could potentially exploit this vulnerability to spawn tasks with elevated privileges.	7.6	More Details
CVE-2021-31984	Power BI Remote Code Execution Vulnerability	7.6	More Details
CVE-2020-12733	Certain Shenzhen PENGLIXIN components on DEPSTECH WiFi Digital Microscope 3, as used by Shekar Endoscope, allow a TELNET connection with the molinkadmin password for the molink account.	7.5	More Details
CVE-2021-20439	IBM Security Access Manager 9.0 and IBM Security Verify Access Docker 10.0.0 stores user credentials in plain clear text which can be read by an unauthorized user.	7.5	More Details
CVE-2021-29725	IBM Secure External Authentication Server 2.4.3.2, 6.0.1, 6.0.2 and IBM Secure Proxy 3.4.3.2, 6.0.1, 6.0.2 could allow a remote user to consume resources causing a denial of service due to a resource leak.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12731	The MagicMotion Flamingo 2 application for Android stores data on an sdcard under com.vt.magicmotion/files/Pictures, whence it can be read by other applications.	7.5	More Details
CVE-2021-20497	IBM Security Verify Access Docker 10.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 197969	7.5	More Details
CVE-2021-3043	A reflected cross-site scripting (XSS) vulnerability exists in the Prisma Cloud Compute web console that enables a remote attacker to execute arbitrary JavaScript code in the browser-based web console while an authenticated administrator is using that web interface. Prisma Cloud Compute SaaS versions were automatically upgraded to the fixed release. No additional action is required for these instances. This issue impacts: Prisma Cloud Compute 20.12 versions earlier than Prisma Cloud Compute 20.12.552; Prisma Cloud Compute 21.04 versions earlier than Prisma Cloud Compute 21.04.439.	7.5	More Details
CVE-2021-20748	Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	7.5	More Details
CVE-2020-23284	Information disclosure in aspx pages in MV's IDCE application v1.0 allows an attacker to copy and paste aspx pages in the end of the URL application that connect into the database which reveals internal and sensitive information without logging into the web application.	7.5	More Details
CVE-2021-22235	Crash in DNP dissector in Wireshark 3.4.0 to 3.4.6 and 3.2.0 to 3.2.14 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-26095	The combination of various cryptographic issues in the session management of FortiMail 6.4.0 through 6.4.4 and 6.2.0 through 6.2.6, including the encryption construction of the session cookie, may allow a remote attacker already in possession of a cookie to possibly reveal and alter or forge its content, thereby escalating privileges.	7.5	More Details
CVE-2021-35054	Minecraft before 1.17.1, when online-mode=false is configured, allows path traversal for deletion of arbitrary JSON files.	7.5	More Details
CVE-2020-22741	An issue was discovered in Xuperchain 3.6.0 that allows for attackers to recover any arbitrary users' private key after obtaining the partial signature in multisignature.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34820	Web Path Directory Traversal in the Novus HTTP Server. The Novus HTTP Server is affected by the Directory Traversal for Arbitrary File Access vulnerability. A remote, unauthenticated attacker using an HTTP GET request may be able to exploit this issue to access sensitive data. The issue was discovered in the NMS (Novus Management System) software through 1.51.2	7.5	More Details
CVE-2021-34676	Basix NEX-Forms through 7.8.7 allows authentication bypass for Excel report generation.	7.5	More Details
CVE-2021-34675	Basix NEX-Forms through 7.8.7 allows authentication bypass for stored PDF reports.	7.5	More Details
CVE-2020-36426	An issue was discovered in Arm Mbed TLS before 2.24.0. mbedtls_x509_crl_parse_der has a buffer over-read (of one byte).	7.5	More Details
CVE-2020-36423	An issue was discovered in Arm Mbed TLS before 2.23.0. A remote attacker can recover plaintext because a certain Lucky 13 countermeasure doesn't properly consider the case of a hardware accelerator.	7.5	More Details
CVE-2020-22650	A memory leak vulnerability in sim-organizer.c of AlienVault Ossim v5 causes a denial of service (DOS) via a system crash triggered by the occurrence of a large number of alarm events.	7.5	More Details
CVE-2021-20109	Due to the Asset Explorer agent not validating HTTPS certificates, an attacker on the network can statically configure their IP address to match the Asset Explorer's Server IP address. This will allow an attacker to send a NEWSCAN request to a listening agent on the network as well as receive the agent's HTTP request verifying its authtoken. In AEAgent.cpp, the agent responding back over HTTP is vulnerable to a Heap Overflow if the POST payload response is too large. The POST payload response is converted to Unicode using vswprintf. This is written to a buffer only 0x2000 bytes big. If POST payload is larger, then heap overflow will occur.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20108	Manage Engine Asset Explorer Agent 1.0.34 listens on port 9000 for incoming commands over HTTPS from Manage Engine Server. The HTTPS certificates are not verified which allows any arbitrary user on the network to send commands over port 9000. While these commands may not be executed (due to authtoken validation), the Asset Explorer agent will reach out to the manage engine server for an HTTP request. During this process, AEAgent.cpp allocates 0x66 bytes using "malloc". This memory is never free-ed in the program, causing a memory leak. Additionally, the instruction sent to aeagent (ie: NEWSCAN, DELTASCAN, etc) is converted to a unicode string, but is never freed. These memory leaks allow a remote attacker to exploit a Denial of Service scenario through repetitively sending these commands to an agent and eventually crashing it the agent due to an out-of-memory condition.	7.5	More Details
CVE-2021-36773	uBlock Origin before 1.36.2 and nMatrix before 4.4.9 support an arbitrary depth of parameter nesting for strict blocking, which allows crafted web sites to cause a denial of service (unbounded recursion that can trigger memory consumption and a loss of all blocking functionality).	7.5	More Details
CVE-2021-36213	HashiCorp Consul and Consul Enterprise 1.9.0 through 1.10.0 default deny policy with a single L7 application-aware intention deny action cancels out, causing the intention to incorrectly fail open, allowing L4 traffic. Fixed in 1.9.8 and 1.10.1.	7.5	More Details
CVE-2021-32574	HashiCorp Consul and Consul Enterprise 1.3.0 through 1.10.0 Envoy proxy TLS configuration does not validate destination service identity in the encoded subject alternative name. Fixed in 1.8.14, 1.9.8, and 1.10.1.	7.5	More Details
CVE-2021-32769	Micronaut is a JVM-based, full stack Java framework designed for building JVM applications. A path traversal vulnerability exists in versions prior to 2.5.9. With a basic configuration, it is possible to access any file from a filesystem, using "/../../" in the URL. This occurs because Micronaut does not restrict file access to configured paths. The vulnerability is patched in version 2.5.9. As a workaround, do not use `**` in mapping, use only `*`, which exposes only flat structure of a directory not allowing traversal. If using Linux, another workaround is to run micronaut in chroot.	7.5	More Details
CVE-2021-35962	Specific page parameters in Dr. ID Door Access Control and Personnel Attendance Management system does not filter special characters. Remote attackers can apply Path Traversal means to download credential files from the system without permission.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34691	iDrive RemotePC before 4.0.1 on Linux allows denial of service. A remote and unauthenticated attacker can disconnect a valid user session by connecting to an ephemeral port.	7.5	More Details
CVE-2021-21818	A hard-coded password vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to a denial of service. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details
CVE-2021-21817	An information disclosure vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details
CVE-2021-0286	A vulnerability in the handling of exceptional conditions in Juniper Networks Junos OS Evolved (EVO) allows an attacker to send specially crafted packets to the device, causing the Advanced Forwarding Toolkit manager (evo-aftmand-bt or evo-aftmand-zx) process to crash and restart, impacting all traffic going through the FPC, resulting in a Denial of Service (DoS). Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Following messages will be logged prior to the crash: Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:32710470974358 label:1089551617 for session:18 probe:35 Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:19241453497049 label:1089551617 for session:18 probe:37 Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:19241453497049 label:1089551617 for session:18 probe:44 Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:32710470974358 label:1089551617 for session:18 probe:47 Feb 2 10:14:39 fpc0 audit[16263]: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=16263 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=11 Feb 2 10:14:39 fpc0 kernel: audit: type=1701 audit(1612260879.272:17): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=16263 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=1 This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0285	An uncontrolled resource consumption vulnerability in Juniper Networks Junos OS on QFX5000 Series and EX4600 Series switches allows an attacker sending large amounts of legitimate traffic destined to the device to cause Interchassis Control Protocol (ICCP) interruptions, leading to an unstable control connection between the Multi-Chassis Link Aggregation Group (MC-LAG) nodes which can in turn lead to traffic loss. Continued receipt of this amount of traffic will create a sustained Denial of Service (DoS) condition. An indication that the system could be impacted by this issue is the following log message: "DDOS_PROTOCOL_VIOLATION_SET: Warning: Host-bound traffic for protocol/exception LOCALNH:aggregate exceeded its allowed bandwidth at fpc <fpc number> for <n> times, started at <timestamp>" This issue affects Juniper Networks Junos OS on QFX5000 Series and EX4600 Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2.	7.5	More Details
CVE-2021-0283	A buffer overflow vulnerability in the TCP/IP stack of Juniper Networks Junos OS allows an attacker to send specific sequences of packets to the device thereby causing a Denial of Service (DoS). By repeatedly sending these sequences of packets to the device, an attacker can sustain the Denial of Service (DoS) condition. The device will abnormally shut down as a result of these sent packets. A potential indicator of compromise will be the following message in the log files: "eventd[13955]: SYSTEM_ABNORMAL_SHUTDOWN: System abnormally shut down" These issue are only triggered by traffic destined to the device. Transit traffic will not trigger these issues. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 16.1 version 16.1R1 and later versions; 16.2 version 16.2R1 and later versions; 17.1 version 17.1R1 and later versions; 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S12; 17.4 version 17.4R1 and later versions; 18.1 versions prior to 18.1R3-S13; 18.2 version 18.2R1 and later versions; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; 21.2 versions prior to 21.2R1-S1, 21.2R2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0282	On Juniper Networks Junos OS devices with Multipath or add-path feature enabled, processing a specific BGP UPDATE can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued receipt and processing of this UPDATE message will create a sustained Denial of Service (DoS) condition. This BGP UPDATE message can propagate to other BGP peers with vulnerable Junos versions on which Multipath or add-path feature is enabled, and cause RPD to crash and restart. This issue affects both IBGP and EBGP deployments in IPv4 or IPv6 network. Junos OS devices that do not have the BGP Multipath or add-path feature enabled are not affected by this issue. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S18; 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S3;	7.5	More Details
CVE-2021-0280	Due to an Improper Initialization vulnerability in Juniper Networks Junos OS on PTX platforms and QFX10K Series with Paradise (PE) chipset-based line cards, ddos-protection configuration changes made from the CLI will not take effect as expected beyond the default DDoS (Distributed Denial of Service) settings in the Packet Forwarding Engine (PFE). This may cause BFD sessions to flap when a high rate of specific packets are received. Flapping of BFD sessions in turn may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms with Paradise (PE) chipset-based line cards: PTX1000, PTX3000 (NextGen), PTX5000, PTX10008, PTX10016 Series and QFX10002 Series. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R3-S5 on PTX Series, QFX10K Series; 18.2 versions prior to 18.2R3-S8 on PTX Series, QFX10K Series; 18.3 versions prior to 18.3R3-S5 on PTX Series, QFX10K Series; 18.4 versions prior to 18.4R2-S8 on PTX Series, QFX10K Series; 19.1 versions prior to 19.1R3-S5 on PTX Series, QFX10K Series; 19.2 versions prior to 19.2R3-S2 on PTX Series, QFX10K Series; 19.3 versions prior to 19.3R3-S2 on PTX Series, QFX10K Series; 19.4 versions prior to 19.4R3-S2 on PTX Series, QFX10K Series; 20.1 versions prior to 20.1R3 on PTX Series, QFX10K Series; 20.2 versions prior to 20.2R2-S3, 20.2R3 on PTX Series, QFX10K Series; 20.3 versions prior to 20.3R2 on PTX Series, QFX10K Series; 20.4 versions prior to 20.4R2 on PTX Series, QFX10K Series.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32770	Gatsby is a framework for building websites. The gatsby-source-wordpress plugin prior to versions 4.0.8 and 5.9.2 leaks .htaccess HTTP Basic Authentication variables into the app.js bundle during build-time. Users who are not initializing basic authentication credentials in the gatsby-config.js are not affected. A patch has been introduced in gatsby-source-wordpress@4.0.8 and gatsby-source-wordpress@5.9.2 which mitigates the issue by filtering all variables specified in the `auth: { }` section. Users that depend on this functionality are advised to upgrade to the latest release of gatsby-source-wordpress, run `gatsby clean` followed by a `gatsby build`. One may manually edit the app.js file post-build as a workaround.	7.5	More Details
CVE-2021-3649	chatwoot is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-32751	Gradle is a build tool with a focus on build automation. In versions prior to 7.2, start scripts generated by the `application` plugin and the `gradlew` script are both vulnerable to arbitrary code execution when an attacker is able to change environment variables for the user running the script. This may impact those who use `gradlew` on Unix-like systems or use the scripts generated by Gradle in thieir application on Unix-like systems. For this vulnerability to be exploitable, an attacker needs to be able to set the value of particular environment variables and have those environment variables be seen by the vulnerable scripts. This issue has been patched in Gradle 7.2 by removing the use of `eval` and requiring the use of the `bash` shell. There are a few workarounds available. For CI/CD systems using the Gradle build tool, one may ensure that untrusted users are unable to change environment variables for the user that executes `gradlew`. If one is unable to upgrade to Gradle 7.2, one may generate a new `gradlew` script with Gradle 7.2 and use it for older versions of Gradle. Fpplications using start scripts generated by Gradle, one may ensure that untrusted users are unable to change environment variables for the user that executes the start script. A vulnerable start script could be manually patched to remove the use of `eval` or the use of environment variables that affect the application's command-line. If the application is simple enough, one may be able to avoid the use of the start scripts by running the application directly with Java command.	7.5	More Details
CVE-2021-34490	Windows TCP/IP Driver Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34173	An attacker can cause a Denial of Service and kernel panic in v4.2 and earlier versions of Espressif esp32 via a malformed beacon csa frame. The device requires a reboot to recover.	7.5	More Details
CVE-2021-33785	Windows AF_UNIX Socket Provider Denial of Service Vulnerability	7.5	More Details
CVE-2021-0596	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181346550	7.5	More Details
CVE-2021-33772	Windows TCP/IP Driver Denial of Service Vulnerability	7.5	More Details
CVE-2021-35527	Password autocomplete vulnerability in the web application password field of Hitachi ABB Power Grids eSOMS allows attacker to gain access to user credentials that are stored by the browser. This issue affects: Hitachi ABB Power Grids eSOMS version 6.3 and prior versions.	7.5	More Details
CVE-2021-33677	SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 702, 730, 731, 804, 740, 750, 784, expose functions to external which can lead to information disclosure.	7.5	More Details
CVE-2021-33788	Windows LSA Denial of Service Vulnerability	7.5	More Details
CVE-2021-33670	SAP NetWeaver AS for Java (Http Service Monitoring Filter), versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send multiple HTTP requests with different method types thereby crashing the filter and making the HTTP server unavailable to other legitimate users leading to denial of service vulnerability.	7.5	More Details
CVE-2021-36716	A ReDoS (regular expression denial of service) flaw was found in the Segment is-email package before 1.0.1 for Node.js. An attacker that is able to provide crafted input to the isEmail(input) function may cause an application to consume an excessive amount of CPU.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36420	Polipo through 1.1.1, when NDEBUG is omitted, allows denial of service via a reachable assertion during parsing of a malformed Range header. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details
CVE-2021-34476	Bowser.sys Denial of Service Vulnerability	7.5	More Details
CVE-2021-31183	Windows TCP/IP Driver Denial of Service Vulnerability	7.5	More Details
CVE-2020-29147	A SQL injection vulnerability in wy_controlls/wy_side_visitor.php of Wayang-CMS v1.0 allows attackers to obtain sensitive database information.	7.5	More Details
CVE-2021-23407	This affects the package elFinder.Net.Core from 0 and before 1.2.4. The user-controlled file name is not properly sanitized before it is used to create a file system path.	7.5	More Details
CVE-2021-35964	The management page of the Orca HCM digital learning platform does not perform identity verification, which allows remote attackers to execute the management function without logging in, access members' information, modify and delete the courses in system, thus causing users fail to access the learning content.	7.3	More Details
CVE-2021-0441	In onCreate of PermissionActivity.java, there is a possible permission bypass due to Confusing UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174495520	7.3	More Details
CVE-2021-33766	Microsoft Exchange Server Information Disclosure Vulnerability	7.3	More Details
CVE-2021-21819	A code execution vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2021-20533	IBM Security Verify Access Docker 10.0.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 198813	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31196	Microsoft Exchange Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2021-33676	A missing authority check in SAP CRM, versions - 700, 701, 702, 712, 713, 714, could be leveraged by an attacker with high privileges to compromise confidentiality, integrity, or availability of the system.	7.2	More Details
CVE-2020-25206	The web console for Mimosa B5, B5c, and C5x firmware through 2.8.0.2 allows authenticated command injection in the Throughput, WANStats, PhyStats, and QosStats API classes. An attacker with access to a web console account may execute operating system commands on affected devices by sending crafted POST requests to the affected endpoints (/core/api/calls/Throughput.php, /core/api/calls/WANStats.php, /core/api/calls/PhyStats.php, /core/api/calls/QosStats.php). This results in the complete takeover of the vulnerable device. This vulnerability does not occur in the older 1.5.x firmware versions.	7.2	More Details
CVE-2021-34468	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.1	More Details
CVE-2021-22778	Insufficiently Protected Credentials vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause protected derived function blocks to be read or modified by unauthorized users when accessing a project file.	7.1	More Details
CVE-2021-34467	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.1	More Details
CVE-2021-22780	Insufficiently Protected Credentials vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause unauthorized access to a project file protected by a password when this file is shared with untrusted sources. An attacker may bypass the password protection and be able to view and modify a project file.	7.1	More Details
CVE-2021-34449	Win32k Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33751	Storage Spaces Controller Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-34462	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-33774	Windows Event Tracing Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-34448	Scripting Engine Memory Corruption Vulnerability	6.8	More Details
CVE-2021-34497	Windows MSHTML Platform Remote Code Execution Vulnerability	6.8	More Details
CVE-2019-11098	Insufficient input validation in MdeModulePkg in EDKII may allow an unauthenticated user to potentially enable escalation of privilege, denial of service and/or information disclosure via physical access.	6.8	More Details
CVE-2021-36797	In Victron Energy Venus OS through 2.72, root access is granted by default to anyone with physical access to the device. NOTE: the vendor disagrees with the reporter's opinion about an alleged "security best practices" violation	6.8	More Details
CVE-2021-3453	Some Lenovo Notebook, ThinkPad, and Lenovo Desktop systems have BIOS modules unprotected by Intel Boot Guard that could allow an attacker with physical access the ability to write to the SPI flash storage.	6.8	More Details
CVE-2021-32750	MuWire is a file publishing and networking tool that protects the identity of its users by using I2P technology. Users of MuWire desktop client prior to version 0.8.8 can be de-anonymized by an attacker who knows their full ID. An attacker could send a message with a subject line containing a URL with an HTML image tag and the MuWire client would try to fetch that image via clearnet, thus exposing the IP address of the user. The problem is fixed in MuWire 0.8.8. As a workaround, users can disable messaging functionality to prevent other users from sending them malicious messages.	6.8	More Details
CVE-2021-29699	IBM Security Verify Access Docker 10.0.0 could allow a remote priviled user to upload arbitrary files with a dangerous file type that could be excuted by an user. IBM X-Force ID: 200600.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34447	Windows MSHTML Platform Remote Code Execution Vulnerability	6.8	More Details
CVE-2021-34493	Windows Partition Management Driver Elevation of Privilege Vulnerability	6.7	More Details
CVE-2020-25593	Acronis True Image through 2021 on macOS allows local privilege escalation from admin to root due to insecure folder permissions.	6.7	More Details
CVE-2021-35056	Unisys Stealth 5.1 before 5.1.025.0 and 6.0 before 6.0.055.0 has an unquoted Windows search path for a scheduled task. An unintended executable might run.	6.7	More Details
CVE-2021-24022	A buffer overflow vulnerability in FortiAnalyzer CLI 6.4.5 and below, 6.2.7 and below, 6.0.x and FortiManager CLI 6.4.5 and below, 6.2.7 and below, 6.0.x may allow an authenticated, local attacker to perform a Denial of Service attack by running the `diagnose system geoip-city` command with a large ip value.	6.7	More Details
CVE-2021-0585	In beginWrite and beginRead of MessageQueueBase.h, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-184963385	6.7	More Details
CVE-2021-0144	Insecure default variable initialization for the Intel BSSA DFT feature may allow a privileged user to potentially enable an escalation of privilege via local access.	6.7	More Details
CVE-2021-3452	A potential vulnerability in the system shutdown SMI callback function in some ThinkPad models may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2020-23707	A heap-based buffer overflow vulnerability in the function ok_jpg_decode_block_progressive() at ok_jpg.c:1054 of ok-file-formats through 2020-06-26 allows attackers to cause a Denial of Service (DOS) via a crafted jpeg file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34618	A remote denial of service (DoS) vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.18 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.4.x: All versions; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.7 and below; Aruba Instant 8.7.x: 8.7.1.1 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	6.5	More Details
CVE-2020-27379	Cross Site Request Forgery (CSRF) vulnerability in Booking Core - Ultimate Booking System Booking Core 1.7.0 . The CSRF token is not being validated when the request is sent as a GET method. This results in an unauthorized change in the user's email ID, which can later be used to reset the password. The new password will be sent to a modified email ID.	6.5	More Details
CVE-2020-18151	Cross Site Request Forgery (CSRF) vulnerability in ThinkCMF v5.1.0, which can add an admin account.	6.5	More Details
CVE-2021-27847	Division-By-Zero vulnerability in Libvips 8.10.5 in the function vips_eye_point, eye.c#L83, and function vips_mask_point, mask.c#L85.	6.5	More Details
CVE-2021-22867	A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.3 and was fixed in 3.1.3, 3.0.11, and 2.22.17. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2021-33745	Windows DNS Server Denial of Service Vulnerability	6.5	More Details
CVE-2020-12732	DEPSTECH WiFi Digital Microscope 3 has a default SSID of Jetion_xxxxxxxx with a password of 12345678.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34558	The crypto/tls package of Go through 1.16.5 does not properly assert that the type of public key in an X.509 certificate matches the expected type when doing a RSA based key exchange, allowing a malicious TLS server to cause a TLS client to panic.	6.5	More Details
CVE-2021-33680	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes buffer overflow and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	6.5	More Details
CVE-2020-4675	IBM InfoSphere Master Data Management Server 11.6 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 186324.	6.5	More Details
CVE-2020-4980	IBM QRadar SIEM 7.3 and 7.4 uses less secure methods for protecting data in transit between hosts when encrypt host connections is not enabled as well as data at rest. IBM X-Force ID: 192539.	6.5	More Details
CVE-2020-20248	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the memtest process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	6.5	More Details
CVE-2020-20249	Mikrotik RouterOs before stable 6.47 suffers from a memory corruption vulnerability in the resolver process. By sending a crafted packet, an authenticated remote attacker can cause a Denial of Service.	6.5	More Details
CVE-2020-20231	Mikrotik RouterOs through stable version 6.48.3 suffers from a memory corruption vulnerability in the /nova/bin/detnet process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2021-34444	Windows DNS Server Denial of Service Vulnerability	6.5	More Details
CVE-2021-36740	Varnish Cache, with HTTP/2 enabled, allows request smuggling and VCL authorization bypass via a large Content-Length header for a POST request. This affects Varnish Enterprise 6.0.x before 6.0.8r3, and Varnish Cache 5.x and 6.x before 6.5.2, 6.6.x before 6.6.1, and 6.0 LTS before 6.0.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23706	A heap-based buffer overflow vulnerability in the function ok_jpg_decode_block_subsequent_scan() ok_jpg.c:1102 of ok-file-formats through 2020-06-26 allows attackers to cause a Denial of Service (DOS) via a crafted jpeg file.	6.5	More Details
CVE-2020-23705	A global buffer overflow vulnerability in jfif_encode at jfif.c:701 of ffjpeg through 2020-06-22 allows attackers to cause a Denial of Service (DOS) via a crafted jpeg file.	6.5	More Details
CVE-2021-0290	Improper Handling of Exceptional Conditions in Ethernet interface frame processing of Juniper Networks Junos OS allows an attacker to send specially crafted frames over the local Ethernet segment, causing the interface to go into a down state, resulting in a Denial of Service (DoS) condition. The interface does not recover on its own and the FPC must be reset manually. Continued receipt and processing of these frames will create a sustained Denial of Service (DoS) condition. This issue is platform-specific and affects the following platforms and line cards: * MPC7E/8E/9E and MPC10E on MX240, MX480, MX960, MX2008, MX2010, and MX2020 * MX204, MX10003, MX10008, MX10016 * EX9200, EX9251 * SRX4600 No other products or platforms are affected by this vulnerability. An indication of this issue occurring can be seen in the system log messages, as shown below: user@host> show log messages | match "Failed to complete DFE tuning" fpc4 smic_phy_dfe_tuning_state: et-4/1/6 - Failed to complete DFE tuning (count 3) and interface will be in a permanently down state: user@host> show interfaces et-4/1/6 terse Interface Admin Link Proto Local Remote et-4/1/6 up down et-4/1/6.0 up down aenet --> ae101.0 This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S7 on MX Series; 17.1R1 and later versions prior to 17.2R3-S3 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S11, 17.4R3-S1 on MX Series, SRX4600; 18.1 versions prior to 18.1R3-S10 on MX Series, EX9200 Series, SRX4600; 18.2 versions prior to 18.2R3-S3 on MX Series, EX9200 Series, SRX4600; 18.3 versions prior to 18.3R3-S1 on MX Series, EX9200 Series, SRX4600; 18.4 versions prior to 18.4R2-S3, 18.4R3 on MX Series, EX9200 Series, SRX4600; 19.1 versions prior to 19.1R2-S1, 19.1R3 on MX Series, EX9200 Series, SRX4600; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series, EX9200 Series, SRX4600; 19.3 versions prior to 19.3R2 on MX Series, EX9200 Series, SRX4600. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.	6.5	More Details
CVE-2021-36976	libarchive 3.4.1 through 3.5.1 has a use-after-free in copy_string (called from do_uncompress_block and process_block).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33783	Windows SMB Information Disclosure Vulnerability	6.5	More Details
CVE-2021-34507	Windows Remote Assistance Information Disclosure Vulnerability	6.5	More Details
CVE-2021-33678	A function module of SAP NetWeaver AS ABAP (Reconciliation Framework), versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75B, 75C, 75D, 75E, 75F, allows a high privileged attacker to inject code that can be executed by the application. An attacker could thereby delete some critical information and could make the SAP system completely unavailable.	6.5	More Details
CVE-2021-0287	In a Segment Routing ISIS (SR-ISIS)/MPLS environment, on Juniper Networks Junos OS and Junos OS Evolved devices, configured with ISIS Flexible Algorithm for Segment Routing and sensor-based statistics, a flap of a ISIS link in the network, can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued link flaps will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 19.4 versions prior to 19.4R1-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R2; Juniper Networks Junos OS Evolved: 20.3-EVO versions prior to 20.3R2-EVO; 20.4-EVO versions prior to 20.4R2-EVO. This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO.	6.5	More Details
CVE-2021-0288	A vulnerability in the processing of specific MPLS packets in Juniper Networks Junos OS on MX Series and EX9200 Series devices with Trio-based MPCs (Modular Port Concentrators) may cause FPC to crash and lead to a Denial of Service (DoS) condition. Continued receipt of this packet will sustain the Denial of Service (DoS) condition. This issue only affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2;	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36977	matio (aka MAT File I/O Library) 1.5.20 and 1.5.21 has a heap-based buffer overflow in H5MM_memcpy (called from H5MM_malloc and H5C_load_entry), related to use of HDF5 1.12.0.	6.5	More Details
CVE-2021-0289	When user-defined ARP Policer is configured and applied on one or more Aggregated Ethernet (AE) interface units, a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability between the Device Control Daemon (DCD) and firewall process (dfwd) daemons of Juniper Networks Junos OS allows an attacker to bypass the user-defined ARP Policer. In this particular case the User ARP policer is replaced with default ARP policer. To review the desired ARP Policers and actual state one can run the command "show interfaces <> extensive" and review the output. See further details below. An example output is: show interfaces extensive | match policer Policer: Input: __default_arp_policer__ <<< incorrect if user ARP Policer was applied on an AE interface and the default ARP Policer is displayed Policer: Input: jtac-arp-ae5.317-inet-arp <<< correct if user ARP Policer was applied on an AE interface For all platforms, except SRX Series: This issue affects Juniper Networks Junos OS: All versions 5.6R1 and all later versions prior to 18.4 versions prior to 18.4R2-S9, 18.4R3-S9 with the exception of 15.1 versions 15.1R7-S10 and later versions; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S2; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2; This issue does not affect Juniper Networks Junos OS versions prior to 5.6R1. On SRX Series this issue affects Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.4 versions prior to 19.4R3-S4; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S2; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. This issue does not affect 18.4 versions prior to 18.4R1 on SRX Series. This issue does not affect Junos OS Evolved.	6.5	More Details
CVE-2021-33213	An SSRF vulnerability in the "Upload from URL" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to retrieve HTTP and FTP files from the internal server network by inserting an internal address.	6.5	More Details
CVE-2021-34499	Windows DNS Server Denial of Service Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0291	An Exposure of System Data vulnerability in Juniper Networks Junos OS and Junos OS Evolved, where a sensitive system-level resource is not being sufficiently protected, allows a network-based unauthenticated attacker to send specific traffic which partially reaches this resource. A high rate of specific traffic may lead to a partial Denial of Service (DoS) as the CPU utilization of the RE is significantly increased. The SNMP Agent Extensibility (agentx) process should only be listening to TCP port 705 on the internal routing instance. External connections destined to port 705 should not be allowed. This issue affects: Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R2. Juniper Networks Junos OS Evolved versions prior to 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 13.2R1.	6.5	More Details
CVE-2021-20537	IBM Security Verify Access Docker 10.0.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID:198918	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0292	An Uncontrolled Resource Consumption vulnerability in the ARP daemon (arpd) and Network Discovery Protocol (ndp) process of Juniper Networks Junos OS Evolved allows a malicious attacker on the local network to consume memory resources, ultimately resulting in a Denial of Service (DoS) condition. Link-layer functions such as IPv4 and/or IPv6 address resolution may be impacted, leading to traffic loss. The processes do not recover on their own and must be manually restarted. Changes in memory usage can be monitored using the following shell commands (header shown for clarity): user@router:/var/log# ps aux | grep arpd USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 31418 59.0 0.7 *5702564* 247952 ? xxx /usr/sbin/arpd --app-name arpd -I object_select --shared-objects-mode 3 user@router:/var/log# ps aux | grep arpd USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 31418 49.1 1.0 *5813156* 351184 ? xxx /usr/sbin/arpd --app-name arpd -I object_select --shared-objects-mode 3 Memory usage can be monitored for the ndp process in a similar fashion: user@router:/var/log# ps aux | grep ndp USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 14935 0.0 0.1 *5614052* 27256 ? Ssl Jun15 0:17 /usr/sbin/ndp -I no_tab_chk,object_select --app-name ndp --shared-obje user@router:/var/log# ps aux | grep ndp USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 14935 0.0 0.1 *5725164* 27256 ? Ssl Jun15 0:17 /usr/sbin/ndp -I no_tab_chk,object_select --app-name ndp --shared-obje This issue affects Juniper Networks Junos OS Evolved: 19.4 versions prior to 19.4R2-S3-EVO; 20.1 versions prior to 20.1R2-S4-EVO; all versions of 20.2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.4R2-EVO.	6.5	More Details
CVE-2021-33681	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes out of bounds write and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	6.5	More Details
CVE-2020-20230	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the sshd process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	6.5	More Details
CVE-2021-33211	A Directory Traversal vulnerability in the Unzip feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to write files to arbitrary directories via relative paths in ZIP archives.	6.5	More Details
CVE-2021-3614	A vulnerability was reported on some Lenovo Notebook systems that could allow an attacker with physical access to elevate privileges under certain conditions during a BIOS update performed by Lenovo Vantage.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32667	TYPO3 is an open source PHP based web content management system. Versions 9.0.0 through 9.5.28, 10.0.0 through 10.4.17, and 11.0.0 through 11.3.0 have a cross-site scripting vulnerability. When _Page TSconfig_ settings are not properly encoded, corresponding page preview module (_Web>View_) is vulnerable to persistent cross-site scripting. A valid backend user account is needed to exploit this vulnerability. TYPO3 versions 9.5.29, 10.4.18, 11.3.1 contain a patch for this issue.	6.4	More Details
CVE-2021-32668	TYPO3 is an open source PHP based web content management system. Versions 9.0.0 through 9.5.28, 10.0.0 through 10.4.17, and 11.0.0 through 11.3.0 have a cross-site scripting vulnerability. When error messages are not properly encoded, the components _QueryGenerator_ and _QueryView_ are vulnerable to both reflected and persistent cross-site scripting. A valid backend user account having administrator privileges is needed to exploit this vulnerability. TYPO3 versions 9.5.29, 10.4.18, 11.3.1 contain a patch for this issue.	6.4	More Details
CVE-2020-29499	Dell EMC PowerStore versions prior to 1.0.3.0.5.006 contain an OS Command Injection vulnerability in PowerStore X environment . A locally authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS command on the PowerStore underlying OS. Exploiting may lead to a system take over by an attacker.	6.4	More Details
CVE-2021-32669	TYPO3 is an open source PHP based web content management system. Versions 9.0.0 through 9.5.28, 10.0.0 through 10.4.17, and 11.0.0 through 11.3.0 have a cross-site scripting vulnerability. When settings for _backend layouts_ are not properly encoded, the corresponding grid view is vulnerable to persistent cross-site scripting. A valid backend user account is needed to exploit this vulnerability. TYPO3 versions 9.5.29, 10.4.18, 11.3.1 contain a patch for this vulnerability.	6.4	More Details
CVE-2021-33755	Windows Hyper-V Denial of Service Vulnerability	6.3	More Details
CVE-2021-34500	Windows Kernel Memory Information Disclosure Vulnerability	6.3	More Details
CVE-2021-22125	An instance of improper neutralization of special elements in the sniffer module of FortiSandbox before 3.2.2 may allow an authenticated administrator to execute commands on the underlying system's shell via altering the content of its configuration file.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33765	Windows Installer Spoofing Vulnerability	6.2	More Details
CVE-2021-36771	Zoho ManageEngine ADManager Plus before 7110 allows reflected XSS.	6.1	More Details
CVE-2020-29146	A cross site scripting (XSS) vulnerability in index.php of Wayang-CMS v1.0 allows attackers to execute arbitrary web scripts or HTML via a constructed payload created by adding the X-Forwarded-For field to the header.	6.1	More Details
CVE-2021-36772	Zoho ManageEngine ADManager Plus before 7110 allows stored XSS.	6.1	More Details
CVE-2021-35966	The specific function of the Orca HCM digital learning platform does not filter input parameters properly, which causing the URL can be redirected to any website. Remote attackers can use the vulnerability to execute phishing attacks.	6.1	More Details
CVE-2021-34817	A Cross-Site Scripting (XSS) issue in the chat component of Etherpad 1.8.13 allows remote attackers to inject arbitrary JavaScript or HTML by importing a crafted pad.	6.1	More Details
CVE-2021-35043	OWASP AntiSamy before 1.6.4 allows XSS via HTML attributes when using the HTML output serializer (XHTML is not affected). This was demonstrated by a javascript: URL with &#00058 as the replacement for the : character.	6.1	More Details
CVE-2021-3279	sz.chat version 4 allows injection of web scripts and HTML in the message box.	6.1	More Details
CVE-2021-24452	The W3 Total Cache WordPress plugin before 2.1.5 was affected by a reflected Cross-Site Scripting (XSS) issue within the "extension" parameter in the Extensions dashboard, when the 'Anonymously track usage to improve product quality' setting is enabled, as the parameter is output in a JavaScript context without proper escaping. This could allow an attacker, who can convince an authenticated admin into clicking a link, to run malicious JavaScript within the user's web browser, which could lead to full site compromise.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24436	The W3 Total Cache WordPress plugin before 2.1.4 was vulnerable to a reflected Cross-Site Scripting (XSS) security vulnerability within the "extension" parameter in the Extensions dashboard, which is output in an attribute without being escaped first. This could allow an attacker, who can convince an authenticated admin into clicking a link, to run malicious JavaScript within the user's web browser, which could lead to full site compromise.	6.1	More Details
CVE-2021-32774	DataDump is a MediaWiki extension that provides dumps of wikis. Prior to commit 67a82b76e186925330b89ace9c5fd893a300830b, DataDump had no protection against CSRF attacks so requests to generate or delete dumps could be forged. The vulnerability was patched in commit 67a82b76e186925330b89ace9c5fd893a300830b. There are no known workarounds. You must completely disable DataDump.	6.1	More Details
CVE-2020-18145	Cross Site Scripting (XSS) vulnerability in umeditor v1.2.3 via /public/common/umeditor/php/getcontent.php.	6.1	More Details
CVE-2021-31961	Windows InstallService Elevation of Privilege Vulnerability	6.1	More Details
CVE-2021-36755	Nightscout Web Monitor (aka cgm-remote-monitor) 14.2.2 allows XSS via a crafted X-Forwarded-For header.	6.1	More Details
CVE-2021-21799	Cross-site scripting vulnerabilities exist in the telnet_form.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). If a user visits a specially crafted URL, it can lead to arbitrary JavaScript code execution in the context of the targeted user’s browser. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2021-27517	Foxit PDF SDK For Web through 7.5.0 allows XSS. There is arbitrary JavaScript code execution in the browser if a victim uploads a malicious PDF document containing embedded JavaScript code that abuses app.alert (in the Acrobat JavaScript API).	6.1	More Details
CVE-2021-21800	Cross-site scripting vulnerabilities exist in the ssh_form.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). If a user visits a specially crafted URL, it can lead to arbitrary JavaScript code execution in the context of the targeted user’s browser. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25205	The web console for Mimosa B5, B5c, and C5x firmware through 2.8.0.2 is vulnerable to stored XSS in the set_banner() function of /var/www/core/controller/index.php. An unauthenticated attacker may set the contents of the /mnt/jffs2/banner.txt file, stored on the device's filesystem, to contain arbitrary JavaScript. The file contents are then used as part of a welcome/banner message presented to unauthenticated users who visit the login page for the web console. This vulnerability does not occur in the older 1.5.x firmware versions.	6.1	More Details
CVE-2021-21801	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	6.1	More Details
CVE-2021-21802	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	6.1	More Details
CVE-2021-20784	HTTP header injection vulnerability in Everything version 1.0, 1.1, and 1.2 except the Lite version may allow a remote attacker to inject an arbitrary script or alter the website that uses the product.	6.1	More Details
CVE-2021-21803	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	6.1	More Details
CVE-2021-32773	Racket is a general-purpose programming language and an ecosystem for language-oriented programming. In versions prior to 8.2, code evaluated using the Racket sandbox could cause system modules to incorrectly use attacker-created modules instead of their intended dependencies. This could allow system functions to be controlled by the attacker, giving access to facilities intended to be restricted. This problem is fixed in Racket version 8.2. A workaround is available, depending on system settings. For systems that provide arbitrary Racket evaluation, external sandboxing such as containers limit the impact of the problem. For multi-user evaluation systems, such as the `handin-server` system, it is not possible to work around this problem and upgrading is required.	6.1	More Details
CVE-2021-3135	An issue was discovered in the tagDiv Newspaper theme 10.3.9.1 for WordPress. It allows XSS via the wp-admin/admin-ajax.php td_block_id parameter in a td_ajax_block API call.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3647	URI.js is vulnerable to URL Redirection to Untrusted Site	6.1	More Details
CVE-2021-34617	A remote cross-site scripting (XSS) vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.13 and below; Aruba Instant 6.5.x: 6.5.4.13 and below; Aruba Instant 8.3.x: 8.3.0.7 and below; Aruba Instant 8.4.x: 8.4.0.5 and below; Aruba Instant 8.5.x: 8.5.0.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	6.1	More Details
CVE-2021-32749	fail2ban is a daemon to ban hosts that cause multiple authentication errors. In versions 0.9.7 and prior, 0.10.0 through 0.10.6, and 0.11.0 through 0.11.2, there is a vulnerability that leads to possible remote code execution in the mailing action mail-whois. Command `mail` from mailutils package used in mail actions like `mail-whois` can execute command if unescaped sequences (`\n~`) are available in "foreign" input (for instance in whois output). To exploit the vulnerability, an attacker would need to insert malicious characters into the response sent by the whois server, either via a MITM attack or by taking over a whois server. The issue is patched in versions 0.10.7 and 0.11.3. As a workaround, one may avoid the usage of action `mail-whois` or patch the vulnerability manually.	6.1	More Details
CVE-2021-34821	Cross Site Scripting (XSS) vulnerability exists in AAT Novus Management System through 1.51.2. The WebUI has wrong HTTP 404 error handling implemented. A remote, unauthenticated attacker may be able to exploit the issue by sending malicious HTTP requests to non-existing URIs. The value of the URL path filename is copied into the HTML document as plain text tags.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0295	A vulnerability in the Distance Vector Multicast Routing Protocol (DVMRP) of Juniper Networks Junos OS on the QFX10K Series switches allows an attacker to trigger a packet forwarding loop, leading to a partial Denial of Service (DoS). The issue is caused by DVMRP packets looping on a multi-homed Ethernet Segment Identifier (ESI) when VXLAN is configured. DVMRP packets received on a multi-homed ESI are sent to the peer, and then incorrectly forwarded out the same ESI, violating the split horizon rule. This issue only affects QFX10K Series switches, including the QFX10002, QFX10008, and QFX10016. Other products and platforms are unaffected by this vulnerability. This issue affects Juniper Networks Junos OS on QFX10K Series: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 version 18.2R1 and later versions; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2.	6.1	More Details
CVE-2021-0281	On Juniper Networks Junos OS devices configured with BGP origin validation using Resource Public Key Infrastructure (RPKI) receipt of a specific packet from the RPKI cache server may cause routing process daemon (RPD) to crash and restart, creating a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R2-S2-EVO.	5.9	More Details
CVE-2021-33764	Windows Key Distribution Center Information Disclosure Vulnerability	5.9	More Details
CVE-2021-34466	Windows Hello Security Feature Bypass Vulnerability	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36429	Variant_encodeJson in open62541 1.x before 1.0.4 has an out-of-bounds write for a large recursion depth.	5.5	More Details
CVE-2021-0588	In processInboundMessage of MceStateMachine.java, there is a possible SMS disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-177238342	5.5	More Details
CVE-2021-0518	In Wi-Fi, there is a possible leak of location-sensitive data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-176541017	5.5	More Details
CVE-2021-36373	When reading a specially crafted TAR archive an Apache Ant build can be made to allocate large amounts of memory that finally leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	5.5	More Details
CVE-2021-0601	In encodeFrames of avc_enc_fuzzer.cpp, there is a possible out of bounds write due to a double free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-180643802	5.5	More Details
CVE-2021-0599	In scheduleTimeoutLocked of NotificationRecord.java, there is a possible disclosure of a sensitive identifier via broadcasted intent due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175614289	5.5	More Details
CVE-2021-33910	basic/unit-name.c in systemd prior to 246.15, 247.8, 248.5, and 249.1 has a Memory Allocation with an Excessive Size Value (involving strdupa and alloca for a pathname controlled by a local attacker) that results in an operating system crash.	5.5	More Details
CVE-2021-36374	When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amounts of memory that leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Commonly used derived formats from ZIP archives are for instance JAR files and many office files. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0597	In notifyProfileAdded and notifyProfileRemoved of SipService.java, there is a possible way to retrieve SIP account names due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176496502	5.5	More Details
CVE-2021-22318	A component of the HarmonyOS 2.0 has a Null Pointer Dereference Vulnerability. Local attackers may exploit this vulnerability to cause system denial of service.	5.5	More Details
CVE-2020-36427	GNOME gThumb before 3.10.1 allows an application crash via a malformed JPEG image.	5.5	More Details
CVE-2021-36980	Open vSwitch (aka openvswitch) 2.11.0 through 2.15.0 has a use-after-free in decode_NXAST_RAW_ENCAP (called from ofpact_decode and ofpacts_decode) during the decoding of a RAW_ENCAP action.	5.5	More Details
CVE-2021-36979	Unicorn Engine 1.0.2 has an out-of-bounds write in tb_flush_armeb (called from cpu_arm_exec_armeb and tcg_cpu_exec_armeb).	5.5	More Details
CVE-2021-36978	QPDF 9.x through 9.1.1 and 10.x through 10.0.4 has a heap-based buffer overflow in Pl_ASCII85Decoder::write (called from Pl_AES_PDF::flush and Pl_AES_PDF::finish) when a certain downstream write fails.	5.5	More Details
CVE-2021-32013	SheetJS and SheetJS Pro through 0.16.9 allows attackers to cause a denial of service (memory consumption) via a crafted .xlsx document that is mishandled when read by xlsx.js (issue 2 of 2).	5.5	More Details
CVE-2020-36431	Unicorn Engine 1.0.2 has an out-of-bounds write in helper_wfe_arm.	5.5	More Details
CVE-2021-32014	SheetJS and SheetJS Pro through 0.16.9 allows attackers to cause a denial of service (CPU consumption) via a crafted .xlsx document that is mishandled when read by xlsx.js.	5.5	More Details
CVE-2021-34689	iDrive RemotePC before 7.6.48 on Windows allows information disclosure. A locally authenticated attacker can read the system's Personal Key in world-readable %PROGRAMDATA% log files.	5.5	More Details
CVE-2021-32012	SheetJS and SheetJS Pro through 0.16.9 allows attackers to cause a denial of service (memory consumption) via a crafted .xlsx document that is mishandled when read by xlsx.js (issue 1 of 2).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34509	Storage Spaces Controller Information Disclosure Vulnerability	5.5	More Details
CVE-2021-33763	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2021-33760	Media Foundation Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0293	A vulnerability in Juniper Networks Junos OS caused by Missing Release of Memory after Effective Lifetime leads to a memory leak each time the CLI command 'show system connections extensive' is executed. The amount of memory leaked on each execution depends on the number of TCP connections from and to the system. Repeated execution will cause more memory to leak and eventually daemons that need to allocate additionally memory and ultimately the kernel to crash, which will result in traffic loss. Continued execution of this command will cause a sustained Denial of Service (DoS) condition. An administrator can use the following CLI command to monitor for increase in memory consumption of the netstat process, if it exists: user@junos> show system processes extensive | match "username|netstat" PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 21181 root 100 0 5458M 4913M CPU3 2 0:59 97.27% netstat The following log message might be observed if this issue happens: kernel: %KERN-3: pid 21181 (netstat), uid 0, was killed: out of swap space This issue affects Juniper Networks Junos OS 18.2 versions prior to 18.2R2-S8, 18.2R3-S7. 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2; This issue does not affect Juniper Networks Junos OS versions prior to 18.2R1.	5.5	More Details
CVE-2021-33782	Windows Authenticode Spoofing Vulnerability	5.5	More Details
CVE-2021-34491	Win32k Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34496	Windows GDI Information Disclosure Vulnerability	5.5	More Details
CVE-2021-34440	GDI+ Information Disclosure Vulnerability	5.5	More Details
CVE-2021-34454	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2021-22782	Missing Encryption of Sensitive Data vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause an information leak allowing disclosure of network and process information, credentials or intellectual property when an attacker can access a project file.	5.5	More Details
CVE-2021-34457	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2021-22781	Insufficiently Protected Credentials vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause a leak of SMTP credential used for mailbox authentication when an attacker can access a project file.	5.5	More Details
CVE-2021-0604	In generateFileInfo of BluetoothOppSendFileInfo.java, there is a possible way to share private files over Bluetooth due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179910660	5.5	More Details
CVE-2021-0654	In isRealSnapshot of TaskThumbnailView.java, there is possible data exposure due to a missing permission check. This could lead to local information disclosure from locked profiles with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168802517References: N/A	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27845	A Divide-by-zero vulnerability exists in JasPer Image Coding Toolkit 2.0 in jasper/src/libjasper/jpc/jpc_enc.c	5.5	More Details
CVE-2021-20507	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198235.	5.4	More Details
CVE-2021-36758	1Password Connect server before 1.2 is missing validation checks, permitting users to create Secrets Automation access tokens that can be used to perform privilege escalation. Malicious users authorized to create Secrets Automation access tokens can create tokens that have access beyond what the user is authorized to access, but limited to the existing authorizations of the Secret Automation the token is created in.	5.4	More Details
CVE-2021-26083	Export HTML Report in Atlassian Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.16.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-5323	Dell EMC OpenManage Enterprise (OME) versions prior to 3.2 and OpenManage Enterprise-Modular (OME-M) versions prior to 1.10.00 contain an injection vulnerability. A remote authenticated malicious user with low privileges could potentially exploit this vulnerability to gain access to sensitive information or cause denial-of-service.	5.4	More Details
CVE-2021-36747	Blackboard Learn through 9.1 allows XSS by an authenticated user via the Feedback to Learner form.	5.4	More Details
CVE-2021-33682	SAP Lumira Server version 2.4 does not sufficiently encode user controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. This would allow an attacker with basic level privileges to store a malicious script on SAP Lumira Server. The execution of the script content, by a victim registered on SAP Lumira Server, could compromise the confidentiality and integrity of SAP Lumira content.	5.4	More Details
CVE-2021-36746	Blackboard Learn through 9.1 allows XSS by an authenticated user via the Assignment Instructions HTML editor.	5.4	More Details
CVE-2021-28114	Froala WYSIWYG Editor 3.2.6-1 is affected by XSS due to a namespace confusion during parsing.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5031	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 193738.	5.4	More Details
CVE-2021-33212	A Cross-site scripting (XSS) vulnerability in the "View in Browser" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to inject arbitrary web script or HTML via a crafted SVG image.	5.4	More Details
CVE-2021-28054	An issue was discovered in Centreon-Web in Centreon Platform 20.10.0. A Stored Cross-Site Scripting (XSS) issue in "Configuration > Hosts" allows remote authenticated users to inject arbitrary web script or HTML via the Alias parameter.	5.4	More Details
CVE-2021-29749	IBM Secure External Authentication Server 6.0.2 and IBM Secure Proxy 6.0.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 201777.	5.4	More Details
CVE-2021-26082	The XML Export in Atlassian Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.17.0 allows remote attackers to inject arbitrary HTML or JavaScript via a stored cross site scripting vulnerability.	5.4	More Details
CVE-2021-27338	Faraday Edge before 3.7 allows XSS via the network/create/ page and its network name parameter.	5.4	More Details
CVE-2020-25444	Cross Site Scripting (XSS) vulnerability in Booking Core - Ultimate Booking System Booking Core 1.7.0 via the (1) "About Yourself” section under the “My Profile” page, " (2) “Hotel Policy” field under the “Hotel Details” page, (3) “Pricing code” and “name” fields under the “Manage Tour” page, and (4) all the labels under the “Menu” section.	5.4	More Details
CVE-2021-34687	iDrive RemotePC before 7.6.48 on Windows allows information disclosure. A man in the middle can recover a system's Personal Key when a client attempts to make a LAN connection. The Personal Key is transmitted over the network while only being encrypted via a substitution cipher.	5.3	More Details
CVE-2021-20498	IBM Security Verify Access Docker 10.0.0 reveals version information in HTTP requests that could be used in further attacks against the system. IBM X-Force ID: 197972.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32767	TYPO3 is an open source PHP based web content management system. In versions 9.0.0 through 9.5.27, 10.0.0 through 10.4.17, and 11.0.0 through 11.3.0, user credentials may been logged as plain-text. This occurs when explicitly using log level debug, which is not the default configuration. TYPO3 versions 9.5.28, 10.4.18, 11.3.1 contain a patch for this vulnerability.	5.3	More Details
CVE-2020-12730	MagicMotion Flamingo 2 lacks BLE encryption, enabling data sniffing and packet forgery.	5.3	More Details
CVE-2021-0294	A vulnerability in Juniper Networks Junos OS, which only affects the release 18.4R2-S5, where a function is inconsistently implemented on Juniper Networks Junos QFX5000 Series and EX4600 Series, and if "storm-control enhanced" is configured, can lead to the enhanced storm control filter group not be installed. It will cause storm control not to work hence allowing an attacker to cause high CPU usage or packet loss issues by sending a large amount of broadcast or unknown unicast packets arriving the device. This issue affects Juniper Networks QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, EX4600, and EX4650, and QFX5100 with QFX 5e Series image installed. QFX5130 and QFX5220 are not affected from this issue. This issue affects Juniper Networks Junos OS 18.4R2-S5 on QFX5000 Series and EX4600 Series. No other product or platform is affected by this vulnerability.	5.3	More Details
CVE-2021-33684	SAP NetWeaver AS ABAP and ABAP Platform, versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.84, allows an attacker to send overlong content in the RFC request type thereby crashing the corresponding work process because of memory corruption vulnerability. The work process will attempt to restart itself after the crash and hence the impact on the availability is low.	5.3	More Details
CVE-2021-34519	Microsoft SharePoint Server Information Disclosure Vulnerability	5.3	More Details
CVE-2021-34429	For Eclipse Jetty versions 9.4.37-9.4.42, 10.0.1-10.0.5 & 11.0.1-11.0.5, URIs can be crafted using some encoded characters to access the content of the WEB-INF directory and/or bypass some security constraints. This is a variation of the vulnerability reported in CVE-2021-28164/GHSA-v7ff-8wcx-gmc5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21587	Dell Wyse Management Suite versions 3.2 and earlier contain a full path disclosure vulnerability. A local unauthenticated attacker could exploit this vulnerability in order to obtain the path of files and folders.	5.3	More Details
CVE-2021-34517	Microsoft SharePoint Server Spoofing Vulnerability	5.3	More Details
CVE-2021-26081	REST API in Atlassian Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.16.1 allows remote attackers to enumerate usernames via a Sensitive Data Exposure vulnerability in the `/rest/api/latest/user/avatar/temporary` endpoint.	5.3	More Details
CVE-2021-34451	Microsoft Office Online Server Spoofing Vulnerability	5.3	More Details
CVE-2020-36421	An issue was discovered in Arm Mbed TLS before 2.23.0. Because of a side channel in modular exponentiation, an RSA private key used in a secure enclave could be disclosed.	5.3	More Details
CVE-2021-35967	The directory page parameter of the Orca HCM digital learning platform does not filter special characters. Remote attackers can access the system directory thru Path Traversal without logging in.	5.3	More Details
CVE-2020-36422	An issue was discovered in Arm Mbed TLS before 2.23.0. A side channel allows recovery of an ECC private key, related to mbedtls_ecp_check_pub_priv, mbedtls_pk_parse_key, mbedtls_pk_parse_keyfile, mbedtls_ecp_mul, and mbedtls_ecp_mul_restartable.	5.3	More Details
CVE-2020-36425	An issue was discovered in Arm Mbed TLS before 2.24.0. It incorrectly uses a revocationDate check when deciding whether to honor certificate revocation via a CRL. In some situations, an attacker can exploit this by changing the local clock.	5.3	More Details
CVE-2021-33757	Windows Security Account Manager Remote Protocol Security Feature Bypass Vulnerability	5.3	More Details
CVE-2021-36769	A reordering issue exists in Telegram before 7.8.1 for Android, Telegram before 7.8.3 for iOS, and Telegram Desktop before 2.8.8. An attacker can cause the server to receive messages in a different order than they were sent a client.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33744	Windows Secure Kernel Mode Security Feature Bypass Vulnerability	5.3	More Details
CVE-2021-24447	The WP Image Zoom WordPress plugin before 1.47 did not validate its tab parameter before using it in the include_once() function, leading to a local file inclusion issue in the admin dashboard	5.3	More Details
CVE-2021-32760	containerd is a container runtime. A bug was found in containerd versions prior to 1.4.8 and 1.5.4 where pulling and extracting a specially-crafted container image can result in Unix file permission changes for existing files in the host's filesystem. Changes to file permissions can deny access to the expected owner of the file, widen access to others, or set extended bits like setuid, setgid, and sticky. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process. This bug has been fixed in containerd 1.5.4 and 1.4.8. As a workaround, ensure that users only pull images from trusted sources. Linux security modules (LSMs) like SELinux and AppArmor can limit the files potentially affected by this bug through policies and profiles that prevent containerd from interacting with specific files.	5.0	More Details
CVE-2021-20496	IBM Security Verify Access Docker 10.0.0 could allow an authenticated user to bypass input due to improper input validation. IBM X-Force ID: 197966.	4.9	More Details
CVE-2021-24117	In Apache Teaclave Rust SGX SDK 1.1.3, a side-channel vulnerability in base64 PEM file decoding allows system-level (administrator) attackers to obtain information about secret RSA keys via a controlled-channel and side-channel attack on software running in isolated environments that can be single stepped, especially Intel SGX.	4.9	More Details
CVE-2021-33687	SAP NetWeaver AS JAVA (Enterprise Portal), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50 reveals sensitive information in one of their HTTP requests, an attacker can use this in conjunction with other attacks such as XSS to steal this information.	4.9	More Details
CVE-2021-20511	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 198300.	4.9	More Details
CVE-2021-24119	In Trusted Firmware Mbed TLS 2.24.0, a side-channel vulnerability in base64 PEM file decoding allows system-level (administrator) attackers to obtain information about secret RSA keys via a controlled-channel and side-channel attack on software running in isolated environments that can be single stepped, especially Intel SGX.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24116	In wolfSSL through 4.6.0, a side-channel vulnerability in base64 PEM file decoding allows system-level (administrator) attackers to obtain information about secret RSA keys via a controlled-channel and side-channel attack on software running in isolated environments that can be single stepped, especially Intel SGX.	4.9	More Details
CVE-2021-20524	IBM Security Verify Access Docker 10.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198661.	4.8	More Details
CVE-2021-24482	The Related Posts for WordPress plugin through 2.0.4 does not sanitise its heading_text and CSS settings, allowing high privilege users (admin) to set XSS payloads in them, leading to Stored Cross-Site Scripting issues.	4.8	More Details
CVE-2021-29780	IBM Resilient OnPrem v41.1 of IBM Security SOAR could allow an authenticated user to perform actions that they should not have access to due to improper input validation. IBM X-Force ID: 203085.	4.7	More Details
CVE-2021-33753	Microsoft Bing Search Spoofing Vulnerability	4.7	More Details
CVE-2020-36424	An issue was discovered in Arm Mbed TLS before 2.24.0. An attacker can recover a private key (for RSA or static Diffie-Hellman) via a side-channel attack against generation of base blinding/unblinding values.	4.7	More Details
CVE-2021-34174	A vulnerability exists in Broadcom BCM4352 and BCM43684 chips. Any wireless router using BCM4352 and BCM43684 will be affected, such as ASUS AX6100. An attacker may cause a Denial of Service (DoS) to any device connected to BCM4352 or BCM43684 routers via an association or reassociation frame.	4.6	More Details
CVE-2020-12729	MagicMotion Flamingo 2 has a lack of access control for reading from device descriptors.	4.6	More Details
CVE-2021-20510	IBM Security Verify Access Docker 10.0.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 198299	4.4	More Details
CVE-2021-20500	IBM Security Verify Access Docker 10.0.0 could reveal highly sensitive information to a local privileged user. IBM X-Force ID: 197980.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0590	In sendNetworkConditionsBroadcast of NetworkMonitor.java, there is a possible way for a privileged app to receive WiFi BSSID and SSID without location permissions due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-175213041	4.4	More Details
CVE-2021-32763	OpenProject is open-source, web-based project management software. In versions prior to 11.3.3, the `MessagesController` class of OpenProject has a `quote` method that implements the logic behind the Quote button in the discussion forums, and it uses a regex to strip `<pre>` tags from the message being quoted. The `(.|\s)` part can match a space character in two ways, so an unterminated `<pre>` tag containing `n` spaces causes Ruby's regex engine to backtrack to try 2ⁿ states in the NFA. This will result in a Regular Expression Denial of Service. The issue is fixed in OpenProject 11.3.3. As a workaround, one may install the patch manually.	4.3	More Details
CVE-2021-35968	The directory list page parameter of the Orca HCM digital learning platform fails to filter special characters properly. Remote attackers can access the system directory thru Path Traversal with users' privileges.	4.3	More Details
CVE-2021-21816	An information disclosure vulnerability exists in the Syslog functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. An attacker can send an HTTP request to trigger this vulnerability.	4.3	More Details
CVE-2021-33667	Under certain conditions, SAP Business Objects Web Intelligence (BI Launchpad) versions - 420, 430, allows an attacker to access jsp source code, through SDK calls, of Analytical Reporting bundle, a part of the frontend application, which would otherwise be restricted.	4.3	More Details
CVE-2021-33683	SAP Web Dispatcher and Internet Communication Manager (ICM), versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.73, WEBDISP 7.53, 7.73, 7.77, 7.81, 7.82, 7.83, KERNEL 7.21, 7.22, 7.49, 7.53, 7.73, 7.77, 7.81, 7.82, 7.83, process invalid HTTP header. The incorrect handling of the invalid Transfer-Encoding header in a particular manner leads to a possibility of HTTP Request Smuggling attack. An attacker could exploit this vulnerability to bypass web application firewall protection, divert sensitive data such as customer requests, session credentials, etc.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33689	When user with insufficient privileges tries to access any application in SAP NetWeaver Administrator (Administrator applications), version - 7.50, no security audit log is created. Therefore, security audit log Integrity is impacted.	4.3	More Details
CVE-2021-20747	Improper authorization in handler for custom URL scheme vulnerability in Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	4.3	More Details
CVE-2020-29503	Dell EMC PowerStore versions prior to 1.0.3.0.5.xxx contain a file permission Vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to the information disclosure of certain system directory.	4.1	More Details
CVE-2021-20534	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 198814	3.5	More Details
CVE-2021-20478	IBM Cloud Pak System 2.3 could allow a local user in some situations to view the artifacts of another user in self service console. IBM X-Force ID: 197497.	3.3	More Details
CVE-2021-34688	iDrive RemotePC before 7.6.48 on Windows allows information disclosure. A locally authenticated attacker can read an encrypted version of the system's Personal Key in world-readable %PROGRAMDATA% log files. The encryption is done using a hard-coded static key and is therefore reversible by an attacker.	3.3	More Details
CVE-2021-20499	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 197973	2.7	More Details
CVE-2021-20523	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 198660	2.7	More Details