SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 February 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-2021-26753	NeDi 1.9C allows an authenticated user to inject PHP code in the System Files function on the endpoint /System-Files.php via the txt HTTP POST parameter. This allows an attacker to obtain access to the operating system where NeDi is installed and to all application data.	9.9	More Details
CVE-2020-28870	In InoERP 0.7.2, an unauthorized attacker can execute arbitrary code on the server side due to lack of validations in /modules/sys/form_personalization/json_fp.php.	9.8	More Details
CVE-2021-27168	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a 6GFJdY4aAuUKJjdtSn7d password for the rdsadmin account.	9.8	More Details
CVE-2021-27170	An issue was discovered on FiberHome HG6245D devices through RP2613. By default, there are no firewall rules for IPv6 connectivity, exposing the internal management interfaces to the Internet.	9.8	More Details
CVE-2021-27171	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to start a Linux telnetd as root on port 26/tcp by using the CLI interface commands of ddd and shell (or tshell).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27172	An issue was discovered on FiberHome HG6245D devices through RP2613. A hardcoded GEPON password for root is defined inside /etc/init.d/system-config.sh.	9.8	More Details
CVE-2021-27177	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to bypass authentication by sending the decoded value of the GgpoZWxwCmxpc3QKd2hvCg== string to the telnet server.	9.8	More Details
CVE-2020-13576	A code execution vulnerability exists in the WS-Addressing plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-27185	The samba-client package before 4.0.0 for Node.js allows command injection because of the use of process.exec.	9.8	More Details
CVE-2021-22652	Access to the Advantech iView versions prior to v5.7.03.6112 configuration are missing authentication, which may allow an unauthorized attacker to change the configuration and obtain code execution.	9.8	More Details
CVE-2021-22658	Advantech iView versions prior to v5.7.03.6112 are vulnerable to a SQL injection, which may allow an attacker to escalate privileges to 'Administrator'.	9.8	More Details
CVE-2021-25689	An out of bounds write in Teradici PCoIP soft client versions prior to version 20.10.1 could allow an attacker to remotely execute code.	9.8	More Details
CVE-2020-27868	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Qognify Ocularis 5.9.0.395. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of serialized objects provided to the EventCoordinator endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-11257.	9.8	More Details
CVE-2021-22504	Arbitrary code execution vulnerability on Micro Focus Operations Bridge Manager product, affecting versions 10.1x, 10.6x, 2018.05, 2018.11, 2019.05, 2019.11, 2020.05, 2020.10. The vulnerability could allow remote attackers to execute arbitrary code on an OBM server.	9.8	More Details
CVE-2019-25019	LimeSurvey before 4.0.0-RC4 allows SQL injection via the participant model.	9.8	More Details
CVE-2021-27213	config.py in pystemon before 2021-02-13 allows code execution via YAML deserialization because SafeLoader and safe_load are not used.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35775	CITSmart before 9.1.2.23 allows LDAP Injection.	9.8	More Details
CVE-2021-3375	ActivePresenter 6.1.6 is affected by a memory corruption vulnerability that may result in a denial of service (DoS) or arbitrary code execution.	9.8	More Details
CVE-2021-26200	The user area for Library System 1.0 is vulnerable to SQL injection where a user can bypass the authentication and login as the admin user.	9.8	More Details
CVE-2021-26201	The Login Panel of CASAP Automated Enrollment System 1.0 is vulnerable to SQL injection authentication bypass. An attacker can obtain access to the admin panel by injecting a SQL query in the username field of the login page.	9.8	More Details
CVE-2021-26822	Teachers Record Management System 1.0 is affected by a SQL injection vulnerability in 'searchteacher' POST parameter in search-teacher.php. This vulnerability can be exploited by a remote unauthenticated attacker to leak sensitive information and perform code execution attacks.	9.8	More Details
CVE-2021-3239	E-Learning System 1.0 suffers from an unauthenticated SQL injection vulnerability, which allows remote attackers to execute arbitrary code on the hosting web server and gain a reverse shell.	9.8	More Details
CVE-2021-27234	An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. The web application suffers from SQL injection on Adminlog.asp, Archivemsgs.asp, Deletelog.asp, Eventlog.asp, and Evmlog.asp.	9.8	More Details
CVE-2021-27236	An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. getfile.asp allows Unauthenticated Local File Inclusion, which can be leveraged to achieve Remote Code Execution.	9.8	More Details
CVE-2020-24841	PNPSCADA 2.200816204020 allows SQL injection via parameter 'interf' in /browse.jsp. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	9.8	More Details
CVE-2021-25648	Mobile application "Testes de Codigo" 11.4 and prior allows an attacker to gain access to the administrative interface and premium features by tampering the boolean value of parameters "isAdmin" and "isPremium" located on device storage.	9.8	More Details
CVE-2020-35565	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. The login pages bruteforce detection is disabled by default.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27101	Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html. The fixed version is FTA_9_12_380 and later.	9.8	More Details
CVE-2021-27103	Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html. The fixed version is FTA_9_12_416 and later.	9.8	More Details
CVE-2020-28871	Remote code execution in Monitorr v1.7.6m in upload.php allows an unauthorized person to execute arbitrary code on the server-side via an insecure file upload.	9.8	More Details
CVE-2021-27169	An issue was discovered on FiberHome AN5506-04-FA devices with firmware RP2631. There is a gepon password for the gepon account.	9.8	More Details
CVE-2021-27167	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a password of four hexadecimal characters for the admin account. These characters are generated in init_3bb_password in libci_adaptation_layer.so.	9.8	More Details
CVE-2021-27166	An issue was discovered on FiberHome HG6245D devices through RP2613. The password for the enable command is gpon.	9.8	More Details
CVE-2020-36244	The daemon in GENIVI diagnostic log and trace (DLT), is vulnerable to a heap-based buffer overflow that could allow an attacker to remotely execute arbitrary code on the DLT-Daemon (versions prior to 2.18.6).	9.8	More Details
CVE-2021-27135	xterm before Patch #366 allows remote attackers to execute arbitrary code or cause a denial of service (segmentation fault) via a crafted UTF-8 combining character sequence.	9.8	More Details
CVE-2021-27141	An issue was discovered on FiberHome HG6245D devices through RP2613. Credentials in /fhconf/umconfig.txt are obfuscated via XOR with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g key. (The webs binary has details on how XOR is used.)	9.8	More Details
CVE-2021-27143	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / user1234 credentials for an ISP.	9.8	More Details
CVE-2021-27144	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded f~i!b@e#r$h%o^m*esuperadmin / s(f)u_h+glu credentials for an ISP.	9.8	More Details
CVE-2021-27145	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / lnadmin credentials for an ISP.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27146	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / CUadmin credentials for an ISP.	9.8	More Details
CVE-2021-27147	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / admin credentials for an ISP.	9.8	More Details
CVE-2021-27148	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded telecomadmin / nE7jA%5m credentials for an ISP.	9.8	More Details
CVE-2021-27149	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded adminpldt / z6dUABtl270qRxt7a2uGTiw credentials for an ISP.	9.8	More Details
CVE-2021-27150	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded gestiontelebucaramanga / t3l3buc4r4m4ng42013 credentials for an ISP.	9.8	More Details
CVE-2021-27151	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded rootmet / m3tr0r00t credentials for an ISP.	9.8	More Details
CVE-2021-27152	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded awnfibre / fibre@dm!n credentials for an ISP.	9.8	More Details
CVE-2021-27153	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded trueadmin / admintrue credentials for an ISP.	9.8	More Details
CVE-2021-27154	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / G0R2U1P2ag credentials for an ISP.	9.8	More Details
CVE-2021-27155	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 3UJUh2VemEfUtesEchEC2d2e credentials for an ISP.	9.8	More Details
CVE-2021-27165	An issue was discovered on FiberHome HG6245D devices through RP2613. The telnet daemon on port 23/tcp can be abused with the gpon/gpon credentials.	9.8	More Details
CVE-2021-27164	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / aisadmin credentials for an ISP.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27163	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / tele1234 credentials for an ISP.	9.8	More Details
CVE-2021-27162	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / tattoo@home credentials for an ISP.	9.8	More Details
CVE-2021-27161	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 1234 credentials for an ISP.	9.8	More Details
CVE-2021-27160	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / 888888 credentials for an ISP.	9.8	More Details
CVE-2021-27159	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded useradmin / 888888 credentials for an ISP.	9.8	More Details
CVE-2021-27158	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded L1vt1m4eng / 888888 credentials for an ISP.	9.8	More Details
CVE-2021-27157	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 888888 credentials for an ISP.	9.8	More Details
CVE-2021-27156	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains credentials for an ISP that equal the last part of the MAC address of the br0 interface.	9.8	More Details
CVE-2021-27104	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints. The fixed version is FTA_9_12_380 and later.	9.8	More Details
CVE-2021-21019	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to XML injection in the Widgets module. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	9.1	More Details
CVE-2021-3033	An improper verification of cryptographic signature vulnerability exists in the Palo Alto Networks Prisma Cloud Compute console. This vulnerability enables an attacker to bypass signature validation during SAML authentication by logging in to the Prisma Cloud Compute console as any authorized user. This issue impacts: All versions of Prisma Cloud Compute 19.11, Prisma Cloud Compute 20.04, and Prisma Cloud Compute 20.09; Prisma Cloud Compute 20.12 before update 1. Prisma Cloud Compute SaaS version is not impacted by this vulnerability.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20651	Directory traversal vulnerability in ELECOM File Manager all versions allows remote attackers to create an arbitrary file or overwrite an existing file in a directory which can be accessed with the application privileges via unspecified vectors.	9.1	More Details
CVE-2020-29026	A directory traversal vulnerability exists in the file upload function of the GateManager that allows an authenticated attacker with administrative permissions to read and write arbitrary files in the Linux file system. This issue affects: GateManager all versions prior to 9.2c.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13561	An out-of-bounds write vulnerability exists in the TIFF parser of Accusoft ImageGear 19.8. A specially crafted malformed file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-26752	NeDi 1.9C allows an authenticated user to execute operating system commands in the Nodes Traffic function on the endpoint /Nodes-Traffic.php via the md or ag HTTP GET parameter. This allows an attacker to obtain access to the operating system where NeDi is installed and to all application data.	8.8	More Details
CVE-2020-27862	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DVA-2800 and DSL-2888A routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the dhttpd service, which listens on TCP port 8008 by default. When parsing the path parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-10911.	8.8	More Details
CVE-2021-25296	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/windowswmi/windowswmi.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server.	8.8	More Details
CVE-2021-25297	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/switch/switch.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21021	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.8	More Details
CVE-2021-25298	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/cloud-vm/cloud-vm.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server.	8.8	More Details
CVE-2020-27874	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent WeChat 7.0.18. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the WXAM Decoder. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11580.	8.8	More Details
CVE-2020-27866	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6020, R6080, R6120, R6220, R6260, R6700v2, R6800, R6900v2, R7450, JNR3210, WNR2020, Nighthawk AC2100, and Nighthawk AC2400 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the mini_httpd service, which listens on TCP port 80 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-11355.	8.8	More Details
CVE-2021-21017	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.8	More Details
CVE-2020-27864	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 firmware version 1.04B03 WiFi extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HNAP service, which listens on TCP port 80 by default. When parsing the Authorization request header, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10880.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27861	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR Orbi 2.5.1.16 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UA_Parser utility. A crafted Host Name option in a DHCP request can trigger execution of a system call composed from a user-supplied string. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-11076.	8.8	More Details
CVE-2021-0340	In parseNextBox of IsoInterface.java, there is a possible leak of unredacted location information due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-134155286	8.8	More Details
CVE-2020-22425	Centreon 19.10-3.el7 is affected by a SQL injection vulnerability, where an authorized user is able to inject additional SQL queries to perform remote command execution.	8.8	More Details
CVE-2020-24899	Nagios XI 5.7.2 is affected by a remote code execution (RCE) vulnerability. An authenticated user can inject additional commands into normal webapp query.	8.8	More Details
CVE-2020-27865	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 firmware version 1.04B03 WiFi extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the uhttpd service, which listens on TCP port 80 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the device. Was ZDI-CAN-10894.	8.8	More Details
CVE-2021-27201	Endian Firewall Community (aka EFW) 3.3.2 allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in a backup comment.	8.8	More Details
CVE-2021-20403	IBM Security Verify Information Queue 1.0.6 and 1.0.7 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.	8.8	More Details
CVE-2021-21028	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.8	More Details
CVE-2021-26751	NeDi 1.9C allows an authenticated user to perform a SQL Injection in the Monitoring History function on the endpoint /Monitoring-History.php via the det HTTP GET parameter. This allows an attacker to access all the data in the database and obtain access to the NeDi application.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13585	An out-of-bounds write vulnerability exists in the PSD Header processing functionality of Accusoft ImageGear 19.8. A specially crafted malformed file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2020-27869	This vulnerability allows remote attackers to escalate privileges on affected installations of SolarWinds Network Performance Monitor 2020 HF1, NPM: 2020.2. Authentication is required to exploit this vulnerability. The specific flaw exists within the WriteToFile method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges and reset the password for the Admin user. Was ZDI-CAN-11804.	8.8	More Details
CVE-2020-13571	An out-of-bounds write vulnerability exists in the SGI RLE decompression functionality of Accusoft ImageGear 19.8. A specially crafted malformed file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2020-13572	A heap overflow vulnerability exists in the way the GIF parser decodes LZW compressed streams in Accusoft ImageGear 19.8. A specially crafted malformed file can trigger a heap overflow, which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-0325	In ih264d_parse_pslice of ih264d_parse_pslice.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution 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-174238784	8.8	More Details
CVE-2021-20073	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows for cross-site request forgeries.	8.8	More Details
CVE-2021-20074	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows users to escape the provided command line interface and execute arbitrary OS commands.	8.8	More Details
CVE-2021-27232	The RTSPLive555.dll ActiveX control in Pelco Digital Sentry Server 7.18.72.11464 has a SetCameraConnectionParameter stack-based buffer overflow. This can be exploited by a remote attacker to potentially execute arbitrary attacker-supplied code. The victim would have to visit a malicious webpage using Internet Explorer where the exploit could be triggered.	8.8	More Details
CVE-2020-13548	In Foxit Reader 10.1.0.37527, a specially crafted PDF document can trigger reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27229	Mumble before 1.3.4 allows remote code execution if a victim navigates to a crafted URL on a server list and clicks on the Open Webpage text.	8.8	More Details
CVE-2021-21035	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.8	More Details
CVE-2021-21033	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.8	More Details
CVE-2021-21307	Lucee Server is a dynamic, Java based (JSR-223), tag and scripting language used for rapid web application development. In Lucee Admin before versions 5.3.7.47, 5.3.6.68 or 5.3.5.96 there is an unauthenticated remote code exploit. This is fixed in versions 5.3.7.47, 5.3.6.68 or 5.3.5.96. As a workaround, one can block access to the Lucee Administrator.	8.6	More Details
CVE-2021-20987	A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.	8.6	More Details
CVE-2021-22978	On BIG-IP version 16.0.x before 16.0.1, 15.1.x before 15.1.1, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.5, and all 12.1.x and 11.6.x versions, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of BIG-IP if the victim user is granted the admin role. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	8.3	More Details
CVE-2021-23874	Arbitrary Process Execution vulnerability in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and execute arbitrary code bypassing MTP self-defense.	8.2	More Details
CVE-2021-20353	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 194882.	8.2	More Details
CVE-2021-21045	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of the current user.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23882	Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows local administrators to prevent the installation of some ENS files by placing carefully crafted files where ENS will be installed. This is only applicable to clean installations of ENS as the Access Control rules will prevent modification prior to up an upgrade.	8.2	More Details
CVE-2021-21511	Dell EMC Avamar Server, versions 19.3 and 19.4 contain an Improper Authorization vulnerability in the web UI. A remote low privileged attacker could potentially exploit this vulnerability, to gain unauthorized read or modification access to other users' backup data.	8.1	More Details
CVE-2021-20411	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user to impersonate another user on the system due to incorrectly updating the session identifier. IBM X-Force ID: 198191.	8.1	More Details
CVE-2021-27197	DSUtility.dll in Pelco Digital Sentry Server before 7.19.67 has an arbitrary file write vulnerability. The AppendToTextFile method doesn't check if it's being called from the application or from a malicious user. The vulnerability is triggered when a remote attacker crafts an HTML page (e.g., with "OBJECT classid=" and "<SCRIPT language='vbscript'>") to overwrite arbitrary files.	8.1	More Details
CVE-2020-4955	IBM Spectrum Protect Operations Center 7.1 and 8.1could allow a remote attacker to execute arbitrary code on the system, caused by improper parameter validation. By creating an unspecified servlet request with specially crafted input parameters, an attacker could exploit this vulnerability to load a malicious .dll with elevated privileges. IBM X-Force ID: 192155.	8.0	More Details
CVE-2021-21053	Adobe Illustrator version 25.1 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2020-27250	In SoftMaker Software GmbH SoftMaker Office PlanMaker 2021 (Revision 1014), a specially crafted document can cause the document parser to copy data from a particular record type into a static-sized buffer within an object that is smaller than the size used for the copy, which will cause a heap-based buffer overflow at Version/Instance 0x0005 and 0x0016. An attacker can entice the victim to open a document to trigger this vulnerability.	7.8	More Details
CVE-2021-21041	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21040	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2020-13581	In SoftMaker Software GmbH SoftMaker Office PlanMaker 2021 (Revision 1014), a specially crafted document can cause the document parser to copy data from a particular record type into a buffer that is smaller than the size used for the copy which will cause a heap-based buffer overflow. An attacker can entice the victim to open a document to trigger this vulnerability.	7.8	More Details
CVE-2021-21039	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-21038	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-22980	In Edge Client version 7.2.x before 7.2.1.1, 7.1.9.x before 7.1.9.8, and 7.1.x-7.1.8.x before 7.1.8.5, an untrusted search path vulnerability in the BIG-IP APM Client Troubleshooting Utility (CTU) for Windows could allow an attacker to load a malicious DLL library from its current directory. User interaction is required to exploit this vulnerability in that the victim must run this utility on the Windows system. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.8	More Details
CVE-2021-21037	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27860	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.0.1.35811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11727.	7.8	More Details
CVE-2020-28596	A stack-based buffer overflow vulnerability exists in the Objparser::objparse() functionality of Prusa Research PrusaSlicer 2.2.0 and Master (commit 4b040b856). A specially crafted obj file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-21036	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2019-19005	A bitmap double free in main.c in autotrace 0.31.1 allows attackers to cause an unspecified impact via a malformed bitmap image. This may occur after the use-after-free in CVE-2017-9182.	7.8	More Details
CVE-2020-35512	A use-after-free flaw was found in D-Bus Development branch <= 1.13.16, dbus-1.12.x stable branch <= 1.12.18, and dbus-1.10.x and older branches <= 1.10.30 when a system has multiple usernames sharing the same UID. When a set of policy rules references these usernames, D-Bus may free some memory in the heap, which is still used by data structures necessary for the other usernames sharing the UID, possibly leading to a crash or other undefined behaviors	7.8	More Details
CVE-2021-27102	Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call. The fixed version is FTA_9_12_416 and later.	7.8	More Details
CVE-2020-28595	An out-of-bounds write vulnerability exists in the Obj.cpp load_obj() functionality of Prusa Research PrusaSlicer 2.2.0 and Master (commit 4b040b856). A specially crafted obj file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-0327	In getContentProviderImpl of ActivityManagerService.java, there is a possible permission bypass due to non-restored binder identities. This could lead to local escalation of privilege 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-172935267	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0337	In moveInMediaStore of FileSystemProvider.java, there is a possible file exposure due to stale metadata. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-157474195	7.8	More Details
CVE-2021-0332	In bootFinished of SurfaceFlinger.cpp, there is a possible memory corruption due to a use after free. 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-10Android ID: A-169256435	7.8	More Details
CVE-2021-0329	In several native functions called by AdvertiseManager.java, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the Bluetooth server with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-171400004	7.8	More Details
CVE-2021-0328	In onBatchScanReports and deliverBatchScan of GattService.java, there is a possible way to retrieve Bluetooth scan results without permissions due to a missing permission check. 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-11 Android-8.1 Android-9Android ID: A-172670415	7.8	More Details
CVE-2021-0334	In onTargetSelected of ResolverActivity.java, there is a possible settings bypass allowing an app to become the default handler for arbitrary domains. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-163358811	7.8	More Details
CVE-2021-0336	In onReceive of BluetoothPermissionRequest.java, there is a possible permissions bypass due to a mutable PendingIntent. This could lead to local escalation of privilege that bypasses a permission check, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-158219161	7.8	More Details
CVE-2021-0305	In PackageInstaller, there is a possible tapjacking attack due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-154015447	7.8	More Details
CVE-2021-26936	The replay-sorcery program in ReplaySorcery 0.4.0 through 0.5.0, when using the default setuid-root configuration, allows a local attacker to escalate privileges to root by specifying video output paths in privileged locations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0302	In PackageInstaller, there is a possible tapjacking attack due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-155287782	7.8	More Details
CVE-2020-13546	In SoftMaker Software GmbH SoftMaker Office TextMaker 2021 (revision 1014), a specially crafted document can cause the document parser to miscalculate a length used to allocate a buffer, later upon usage of this buffer the application will write outside its bounds resulting in a heap-based buffer overflow. An attacker can entice the victim to open a document to trigger this vulnerability.	7.8	More Details
CVE-2020-11635	The Zscaler Client Connector prior to 3.1.0 did not sufficiently validate RPC clients, which allows a local adversary to execute code with system privileges or perform limited actions for which they did not have privileges.	7.8	More Details
CVE-2021-23876	Bypass Remote Procedure call in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and perform arbitrary file modification as the SYSTEM user potentially causing Denial of Service via executing carefully constructed malware.	7.8	More Details
CVE-2020-35567	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. The software uses a secure password for database access, but this password is shared across instances.	7.8	More Details
CVE-2021-23873	Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and perform arbitrary file deletion as the SYSTEM user potentially causing Denial of Service via manipulating Junction link, after enumerating certain files, at a specific time.	7.8	More Details
CVE-2021-20075	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows for privilege escalation via configd.	7.8	More Details
CVE-2021-0339	In loadAnimation of WindowContainer.java, there is a possible way to keep displaying a malicious app while a target app is brought to the foreground. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-145728687	7.8	More Details
CVE-2021-0330	In add_user_ce and remove_user_ce of storaged.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in storaged with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-170732441	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22973	On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.5, and all 12.1.x versions, JSON parser function does not protect against out-of-bounds memory accesses or writes. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.5	More Details
CVE-2021-27191	The get-ip-range package before 4.0.0 for Node.js is vulnerable to denial of service (DoS) if the range is untrusted input. An attacker could send a large range (such as 128.0.0.0/1) that causes resource exhaustion.	7.5	More Details
CVE-2021-20412	IBM Security Verify Information Queue 1.0.6 and 1.0.7 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: 198192.	7.5	More Details
CVE-2021-27184	Pelco Digital Sentry Server 7.18.72.11464 has an XML External Entity vulnerability (exploitable via the DTD parameter entities technique), resulting in disclosure and retrieval of arbitrary data on the affected node via an out-of-band (OOB) attack. The vulnerability is triggered when input passed to the XML parser is not sanitized while parsing the ControlPointCacheShare.xml file (in a %APPDATA%\Pelco directory) when DSControlPoint.exe is executed.	7.5	More Details
CVE-2021-25690	A null pointer dereference in Teradici PCoIP Soft Client versions prior to 20.07.3 could allow an attacker to crash the software.	7.5	More Details
CVE-2020-35558	An issue was discovered in MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual through 2.11.2. There is an SSRF in the in the MySQL access check, allowing an attacker to scan for open ports and gain some information about possible credentials.	7.5	More Details
CVE-2021-27212	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAndThisUpdateCheck function via a crafted packet, resulting in a denial of service (daemon exit) via a short timestamp. This is related to schema_init.c and checkTime.	7.5	More Details
CVE-2021-22974	On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.6 and all versions of BIG-IQ 7.x and 6.x, an authenticated attacker with access to iControl REST over the control plane may be able to take advantage of a race condition to execute commands with an elevated privilege level. This vulnerability is due to an incomplete fix for CVE-2017-6167. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.5	More Details
CVE-2020-35564	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an outdated and unused component allowing for malicious user input of active code.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0326	In p2p_copy_client_info of p2p.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if the target device is performing a Wi-Fi Direct search, 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-172937525	7.5	More Details
CVE-2021-22977	On BIG-IP version 16.0.0-16.0.1 and 14.1.2.4-14.1.3, cooperation between malicious HTTP client code and a malicious server may cause TMM to restart and generate a core file. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.5	More Details
CVE-2020-13949	In Apache Thrift 0.9.3 to 0.13.0, malicious RPC clients could send short messages which would result in a large memory allocation, potentially leading to denial of service.	7.5	More Details
CVE-2020-5023	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 could allow a remote user to inject arbitrary data iwhich could cause the serivce to crash due to excess resource consumption. IBM X-Force ID: 193659.	7.5	More Details
CVE-2020-24838	An integer overflow has been found in the the latest version of Issuer. The total issuedCount can be zero if the parameter is overly large. An attacker can obtain the private key of the owner issued with a certain 'amount', and the issuedCount can be zero if there is an overflow.	7.5	More Details
CVE-2020-24837	An integer underflow has been found in the latest version of ZCFees. The variables 'currPeriodIdx' and 'lastPeriodExecIdx' are both unsigned integers, and the result of the minus operation may be a negative integer which leads to an underflow. The attackers can modify the current timestamp of the transaction somehow and block the execution of the process function.	7.5	More Details
CVE-2013-20001	An issue was discovered in OpenZFS through 2.0.3. When an NFS share is exported to IPv6 addresses via the sharenfs feature, there is a silent failure to parse the IPv6 address data, and access is allowed to everyone. IPv6 restrictions from the configuration are not applied.	7.5	More Details
CVE-2021-22985	On BIG-IP APM version 16.0.x before 16.0.1.1, under certain conditions, when processing VPN traffic with APM, TMM consumes excessive memory. A malicious, authenticated VPN user may abuse this to perform a DoS attack against the APM. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.5	More Details
CVE-2021-22975	On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, and 14.1.x before 14.1.3.1, under some circumstances, Traffic Management Microkernel (TMM) may restart on the BIG-IP system while passing large bursts of traffic. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27218	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation.	7.5	More Details
CVE-2021-22880	The PostgreSQL adapter in Active Record before 6.1.2.1, 6.0.3.5, 5.2.4.5 suffers from a regular expression denial of service (REDoS) vulnerability. Carefully crafted input can cause the input validation in the `money` type of the PostgreSQL adapter in Active Record to spend too much time in a regular expression, resulting in the potential for a DoS attack. This only impacts Rails applications that are using PostgreSQL along with money type columns that take user input.	7.5	More Details
CVE-2021-22656	Advantech iView versions prior to v5.7.03.6112 are vulnerable to directory traversal, which may allow an attacker to read sensitive files.	7.5	More Details
CVE-2021-27186	Fluent Bit 1.6.10 has a NULL pointer dereference when an flb_malloc return value is not validated by flb_avro.c or http_server/api/v1/metrics.c.	7.5	More Details
CVE-2021-23335	All versions of package is-user-valid are vulnerable to LDAP Injection which can lead to either authentication bypass or information exposure.	7.5	More Details
CVE-2021-27142	An issue was discovered on FiberHome HG6245D devices through RP2613. The web management is done over HTTPS, using a hardcoded private key that has 0777 permissions.	7.5	More Details
CVE-2021-27173	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a telnet?enable=0&key=calculated(BR0_MAC) backdoor API, without authentication, provided by the HTTP server. This will remove firewall rules and allow an attacker to reach the telnet server (used for the CLI).	7.5	More Details
CVE-2021-27174	An issue was discovered on FiberHome HG6245D devices through RP2613. wifi_custom.cfg has cleartext passwords and 0644 permissions.	7.5	More Details
CVE-2021-27175	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_2g.cfg has cleartext passwords and 0644 permissions.	7.5	More Details
CVE-2021-27176	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_5g.cfg has cleartext passwords and 0644 permissions.	7.5	More Details
CVE-2021-27178	An issue was discovered on FiberHome HG6245D devices through RP2613. Some passwords are stored in cleartext in nvram.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22654	Advantech iView versions prior to v5.7.03.6112 are vulnerable to a SQL injection, which may allow an unauthorized attacker to disclose information.	7.5	More Details
CVE-2021-27179	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to crash the telnet daemon by sending a certain 0a 65 6e 61 62 6c 65 0a 02 0a 1a 0a string.	7.5	More Details
CVE-2020-13574	A denial-of-service vulnerability exists in the WS-Security plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2020-13575	A denial-of-service vulnerability exists in the WS-Addressing plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2020-13583	A denial-of-service vulnerability exists in the HTTP Server functionality of Micrium uC-HTTP 3.01.00. A specially crafted HTTP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2020-13577	A denial-of-service vulnerability exists in the WS-Security plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2020-13578	A denial-of-service vulnerability exists in the WS-Security plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-27140	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to find passwords and authentication cookies stored in cleartext in the web.log HTTP logs.	7.5	More Details
CVE-2021-22976	On BIG-IP Advanced WAF and ASM version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.6, and all 12.1.x versions, when the BIG-IP ASM system processes WebSocket requests with JSON payloads, an unusually large number of parameters can cause excessive CPU usage in the BIG-IP ASM bd process. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.5	More Details
CVE-2021-27211	steghide 0.5.1 relies on a certain 32-bit seed value, which makes it easier for attackers to detect hidden data.	7.5	More Details
CVE-2021-27188	The Sovremennye Delovye Tekhnologii FX Aggregator terminal client 1 allows attackers to cause a denial of service (access suspended for five hours) by making five invalid login attempts to a victim's account.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20643	Improper access control vulnerability in ELECOM LD-PS/U1 allows remote attackers to change the administrative password of the affected device by processing a specially crafted request.	7.5	More Details
CVE-2021-27139	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to extract information from the device without authentication by disabling JavaScript and visiting /info.asp.	7.5	More Details
CVE-2021-27219	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.	7.5	More Details
CVE-2021-20986	A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.	7.5	More Details
CVE-2021-0341	In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote 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-171980069	7.5	More Details
CVE-2021-27187	The Sovremennye Delovye Tekhnologii FX Aggregator terminal client 1 stores authentication credentials in cleartext in login.sav when the Save Password box is checked.	7.5	More Details
CVE-2021-23840	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).	7.5	More Details
CVE-2021-20405	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user to perform unauthorized activities due to improper encoding of output. IBM X-Force ID: 196183.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35498	A vulnerability was found in openvswitch. A limitation in the implementation of userspace packet parsing can allow a malicious user to send a specially crafted packet causing the resulting megaflow in the kernel to be too wide, potentially causing a denial of service. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2020-25493	Oclean Mobile Application 2.1.2 communicates with an external website using HTTP so it is possible to eavesdrop the network traffic. The content of HTTP payload is encrypted using XOR with a hardcoded key, which allows for the possibility to decode the traffic.	7.5	More Details
CVE-2021-26939	An information disclosure issue exists in henriquedornas 5.2.17 because an attacker can dump phpMyAdmin SQL content. NOTE: third parties report that this is a site-specific problem	7.5	More Details
CVE-2020-8027	A Insecure Temporary File vulnerability in openldap2 of SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to overwrite arbitrary files and gain access to the openldap2 configuration This issue affects: SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.37.1. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.37.1. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.18.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.9.1.	7.3	More Details
CVE-2021-23878	Clear text storage of sensitive Information in memory vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows a local user to view ENS settings and credentials via accessing process memory after the ENS administrator has performed specific actions. To exploit this, the local user has to access the relevant memory location immediately after an ENS administrator has made a configuration change through the console on their machine	7.3	More Details
CVE-2021-0333	In onCreate of BluetoothPermissionActivity.java, there is a possible permissions bypass due to a tapjacking overlay that obscures the phonebook permissions dialog when a Bluetooth device is connecting. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-168504491	7.3	More Details
CVE-2021-0331	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible overlay attack due to an insecure default value. This could lead to local escalation of privilege and notification access with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-170731783	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0314	In onCreate of UninstallerActivity, there is a possible way to uninstall an all without informed user consent 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-10 Android-11 Android-8.1 Android-9Android ID: A-171221302	7.3	More Details
CVE-2021-21311	Adminer is an open-source database management in a single PHP file. In adminer from version 4.0.0 and before 4.7.9 there is a server-side request forgery vulnerability. Users of Adminer versions bundling all drivers (e.g. `adminer.php`) are affected. This is fixed in version 4.7.9.	7.2	More Details
CVE-2021-21976	vSphere Replication 8.3.x prior to 8.3.1.2, 8.2.x prior to 8.2.1.1, 8.1.x prior to 8.1.2.3 and 6.5.x prior to 6.5.1.5 contain a post-authentication command injection vulnerability which may allow an authenticated admin user to perform a remote code execution.	7.2	More Details
CVE-2020-28337	A directory traversal issue in the Utils/Unzip module in Microweber through 1.1.20 allows an authenticated attacker to gain remote code execution via the backup restore feature. To exploit the vulnerability, an attacker must have the credentials of an administrative user, upload a maliciously constructed ZIP file with file paths including relative paths (i.e., ../../), move this file into the backup directory, and execute a restore on this file.	7.2	More Details
CVE-2020-29142	A SQL injection vulnerability in interface/usergroup/usergroup_admin.php in OpenEMR before 5.0.2.5 allows a remote authenticated attacker to execute arbitrary SQL commands via the schedule_facility parameter when restrict_user_facility=on is in global settings.	7.2	More Details
CVE-2021-20072	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to arbitrarily access and delete files via an authenticated directory traveral.	7.2	More Details
CVE-2020-29143	A SQL injection vulnerability in interface/reports/non_reported.php in OpenEMR before 5.0.2.5 allows a remote authenticated attacker to execute arbitrary SQL commands via the form_code parameter.	7.2	More Details
CVE-2020-29140	A SQL injection vulnerability in interface/reports/immunization_report.php in OpenEMR before 5.0.2.5 allows a remote authenticated attacker to execute arbitrary SQL commands via the form_code parameter.	7.2	More Details
CVE-2020-27871	This vulnerability allows remote attackers to create arbitrary files on affected installations of SolarWinds Orion Platform 2020.2.1. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within VulnerabilitySettings.aspx. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-11902.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22982	On BIG-IP DNS and GTM version 13.1.x before 13.1.0.4, and all versions of 12.1.x and 11.6.x, big3d does not securely handle and parse certain payloads resulting in a buffer overflow. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	7.2	More Details
CVE-2020-29139	A SQL injection vulnerability in interface/main/finder/patient_select.php from library/patient.inc in OpenEMR before 5.0.2.5 allows a remote authenticated attacker to execute arbitrary SQL commands via the searchFields parameter.	7.2	More Details
CVE-2021-25251	The Trend Micro Security 2020 and 2021 families of consumer products are vulnerable to a code injection vulnerability which could allow an attacker to disable the program's password protection and disable protection. An attacker must already have administrator privileges on the machine to exploit this vulnerability.	7.2	More Details
CVE-2020-35734	Sruu.pl in Batflat 1.3.6 allows an authenticated user to perform code injection (and consequently Remote Code Execution) via the input fields of the Users tab. To exploit this, one must login to the administration panel and edit an arbitrary user's data (username, displayed name, etc.). NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.2	More Details
CVE-2020-22427	NagiosXI 5.6.11 is affected by a remote code execution (RCE) vulnerability. An authenticated nagiosadmin user can inject additional commands into a request. NOTE: the vendor disputes whether the CVE and its references are actionable because all technical details are omitted, and the only option is to pay for a subscription service where technical details may be disclosed at an unspecified later time	7.2	More Details
CVE-2021-23337	Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.	7.2	More Details
CVE-2021-21315	The System Information Library for Node.JS (npm package "systeminformation") is an open source collection of functions to retrieve detailed hardware, system and OS information. In systeminformation before version 5.3.1 there is a command injection vulnerability. Problem was fixed in version 5.3.1. As a workaround instead of upgrading, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() ... do only allow strings, reject any arrays. String sanitation works as expected.	7.1	More Details
CVE-2020-29031	An Insecure Direct Object Reference vulnerability exists in the web UI of the GateManager which allows an authenticated attacker to reset the password of any user in its domain or any sub-domain, via escalation of privileges. This issue affects all GateManager versions prior to 9.2c	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27209	In the management interface on TP-Link Archer C5v 1.7_181221 devices, credentials are sent in a base64 format over cleartext HTTP.	7.1	More Details
CVE-2021-20188	A flaw was found in podman before 1.7.0. File permissions for non-root users running in a privileged container are not correctly checked. This flaw can be abused by a low-privileged user inside the container to access any other file in the container, even if owned by the root user inside the container. It does not allow to directly escape the container, though being a privileged container means that a lot of security features are disabled when running the container. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.0	More Details
CVE-2020-27867	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6020, R6080, R6120, R6220, R6260, R6700v2, R6800, R6900v2, R7450, JNR3210, WNR2020, Nighthawk AC2100, and Nighthawk AC2400 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the mini_httpd service, which listens on TCP port 80 by default. When parsing the funjsq_access_token parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-11653.	6.8	More Details
CVE-2021-20648	ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.	6.8	More Details
CVE-2021-20639	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.	6.8	More Details
CVE-2021-20640	Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute an arbitrary OS command via unspecified vectors.	6.8	More Details
CVE-2021-20638	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20335	For MongoDB Ops Manager versions prior to and including 4.2.24 with multiple OM application servers, that have SSL turned on for their MongoDB processes, the upgrade to MongoDB Ops Manager versions prior to and including 4.4.12 triggers a bug where Automation thinks SSL is being turned off, and can disable SSL temporarily for members of the cluster. This issue is temporary and eventually corrects itself after MongoDB Ops Manager instances have finished upgrading to MongoDB Ops Manager 4.4. In addition, customers must be running with clientCertificateMode=OPTIONAL / allowConnectionsWithoutCertificates=true to be impacted*.* Customers upgrading from Ops Manager 4.2.X to 4.2.24 and finally to Ops Manager 4.4.13+ are unaffected by this issue.	6.7	More Details
CVE-2021-23880	Improper Access Control in attribute in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows authenticated local administrator user to perform an uninstallation of the anti-malware engine via the running of a specific command with the correct parameters.	6.7	More Details
CVE-2021-21057	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	6.6	More Details
CVE-2021-23338	This affects all versions of package qlib. The workflow function in cli part of qlib was using an unsafe YAML load function.	6.6	More Details
CVE-2021-20641	Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/RS allows remote attackers to hijack the authentication of administrators via a specially crafted URL. As a result, unintended operations to the device such as changes of the device settings may be conducted.	6.5	More Details
CVE-2021-20646	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-A allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started.	6.5	More Details
CVE-2020-35557	An issue in MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual in all versions through v2.11.2 allows a logged in user to see devices in the account he should not have access to due to improper use of access validation.	6.5	More Details
CVE-2021-20647	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-S allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20650	Cross-site request forgery (CSRF) vulnerability in ELECOM NCC-EWF100RMWH2 allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started.	6.5	More Details
CVE-2021-20637	Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/PR5B allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted URL.	6.5	More Details
CVE-2021-27210	TP-Link Archer C5v 1.7_181221 devices allows remote attackers to retrieve cleartext credentials via [USER_CFG#0,0,0,0,0,0#0,0,0,0,0,0]0,0 to the /cgi?1&5 URI.	6.5	More Details
CVE-2021-20642	Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/RS allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted URL.	6.5	More Details
CVE-2020-27863	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DVA-2800 and DSL-2888A routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the dhttpd service, which listens on TCP port 8008 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10912.	6.5	More Details
CVE-2021-20636	Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/PR5B allows remote attackers to hijack the authentication of administrators via a specially crafted URL. As a result, unintended operations to the device such as changes of the device settings may be conducted.	6.5	More Details
CVE-2021-20635	Improper restriction of excessive authentication attempts in LOGITEC LAN-WH450N/GR allows an attacker in the wireless range of the device to recover PIN and access the network.	6.5	More Details
CVE-2020-9307	Hirschmann OS2, RSP, and RSPE devices before HiOS 08.3.00 allow a denial of service. An unauthenticated, adjacent attacker can cause an infinite loop on one of the HSR ring ports of the device. This effectively breaks the redundancy of the HSR ring. If the attacker can perform the same attack on a second device, the ring is broken into two parts (thus disrupting communication between devices in the different parts).	6.5	More Details
CVE-2020-27870	This vulnerability allows remote attackers to disclose sensitive information on affected installations of SolarWinds Orion Platform 2020.2.1. Authentication is required to exploit this vulnerability. The specific flaw exists within ExportToPDF.aspx. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-11917.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21042	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability that could lead to arbitrary disclosure of information in the memory stack. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	6.5	More Details
CVE-2021-0335	In process of C2SoftHevcDec.cpp, there is a possible out of bounds write due to a use after free. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160346309	6.5	More Details
CVE-2020-13186	An Anti CSRF mechanism was discovered missing in the Teradici Cloud Access Connector v31 and earlier in a specific web form, which allowed an attacker with knowledge of both a machineID and user GUID to modify data if a user clicked a malicious link.	6.5	More Details
CVE-2020-13185	Certain web application pages in the authenticated section of the Teradici Cloud Access Connector prior to v18 were accessible without the need to specify authentication tokens, which allowed an attacker in the ability to execute sensitive functions without credentials.	6.5	More Details
CVE-2020-8031	A Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Open Build Service allows remote attackers to store JS code in markdown that is not properly escaped, impacting confidentiality and integrity. This issue affects: Open Build Service versions prior to 2.10.8.	6.3	More Details
CVE-2020-26299	ftp-srv is an open-source FTP server designed to be simple yet configurable. In ftp-srv before version 4.4.0 there is a path-traversal vulnerability. Clients of FTP servers utilizing ftp-srv hosted on Windows machines can escape the FTP user's defined root folder using the expected FTP commands, for example, CWD and UPDR. When windows separators exist within the path (`\`), `path.resolve` leaves the upper pointers intact and allows the user to move beyond the root folder defined for that user. We did not take that into account when creating the path resolve function. The issue is patched in version 4.4.0 (commit 457b859450a37cba10ff3c431eb4aa67771122e3).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21316	less-openui5 is an npm package which enables building OpenUI5 themes with Less.js. In less-openui5 before version 0.10., when processing theming resources (i.e. `*.less` files) with less-openui5 that originate from an untrusted source, those resources might contain JavaScript code which will be executed in the context of the build process. While this is a feature of the Less.js library it is an unexpected behavior in the context of OpenUI5 and SAPUI5 development. Especially in the context of UI5 Tooling which relies on less-openui5. An attacker might create a library or theme-library containing a custom control or theme, hiding malicious JavaScript code in one of the .less files. Refer to the referenced GHSA-3crj-w4f5-gwh4 for examples. Starting with Less.js version 3.0.0, the Inline JavaScript feature is disabled by default. less-openui5 however currently uses a fork of Less.js v1.6.3. Note that disabling the Inline JavaScript feature in Less.js versions 1.x, still evaluates code has additional double codes around it. We decided to remove the inline JavaScript evaluation feature completely from the code of our Less.js fork. This fix is available in less-openui5 version 0.10.0.	6.3	More Details
CVE-2021-21055	Adobe Dreamweaver versions 21.0 (and earlier) and 20.2 (and earlier) is affected by an untrusted search path vulnerability that could result in information disclosure. An attacker with physical access to the system could replace certain configuration files and dynamic libraries that Dreamweaver references, potentially resulting in information disclosure.	6.2	More Details
CVE-2020-35560	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an unauthenticated open redirect in the redirect.php.	6.1	More Details
CVE-2021-22979	On BIG-IP version 16.0.x before 16.0.1, 15.1.x before 15.1.1, 14.1.x before 14.1.2.8, 13.1.x before 13.1.3.5, and all 12.1.x versions, a reflected Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility when Fraud Protection Service is provisioned and allows an attacker to execute JavaScript in the context of the current logged-in user. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	6.1	More Details
CVE-2021-22881	The Host Authorization middleware in Action Pack before 6.1.2.1, 6.0.3.5 suffers from an open redirect vulnerability. Specially crafted `Host` headers in combination with certain "allowed host" formats can cause the Host Authorization middleware in Action Pack to redirect users to a malicious website. Impacted applications will have allowed hosts with a leading dot. When an allowed host contains a leading dot, a specially crafted `Host` header can be used to redirect to a malicious website.	6.1	More Details
CVE-2021-25299	Nagios XI version xi-5.7.5 is affected by cross-site scripting (XSS). The vulnerability exists in the file /usr/local/nagiosxi/html/admin/sshterm.php due to improper sanitization of user-controlled input. A maliciously crafted URL, when clicked by an admin user, can be used to steal his/her session cookies or it can be chained with the previous bugs to get one-click remote command execution (RCE) on the Nagios XI server.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22984	On BIG-IP Advanced WAF and ASM version 15.1.x before 15.1.0.2, 15.0.x before 15.0.1.4, 14.1.x before 14.1.2.5, 13.1.x before 13.1.3.4, 12.1.x before 12.1.5.2, and 11.6.x before 11.6.5.2, when receiving a unauthenticated client request with a maliciously crafted URI, a BIG-IP Advanced WAF or ASM virtual server configured with a DoS profile with Proactive Bot Defense (versions prior to 14.1.0), or a Bot Defense profile (versions 14.1.0 and later), may subject clients and web servers to Open Redirection attacks. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	6.1	More Details
CVE-2020-24842	PNPSCADA 2.200816204020 allows cross-site scripting (XSS), which can execute arbitrary JavaScript in the victim's browser.	6.1	More Details
CVE-2021-26929	An XSS issue was discovered in Horde Groupware Webmail Edition through 5.2.22 (where the Horde_Text_Filter library before 2.3.7 is used). The attacker can send a plain text e-mail message, with JavaScript encoded as a link or email that is mishandled by preProcess in Text2html.php, because bespoke use of \x00\x00\x00 and \x01\x01\x01 interferes with XSS defenses.	6.1	More Details
CVE-2020-36236	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the ViewWorkflowSchemes.jspa and ListWorkflows.jspa endpoints. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.15.0.	6.1	More Details
CVE-2021-21310	NextAuth.js (next-auth) is am open source authentication solution for Next.js applications. In next-auth before version 3.3.0 there is a token verification vulnerability. Implementations using the Prisma database adapter in conjunction with the Email provider are impacted. Implementations using the Email provider with the default database adapter are not impacted. Implementations using the Prisma database adapter but not using the Email provider are not impacted. The Prisma database adapter was checking the verification token, but was not verifying the email address associated with that token. This made it possible to use a valid token to sign in as another user when using the Prima adapter in conjunction with the Email provider. This issue is specific to the community supported Prisma adapter. This issue is fixed in version 3.3.0.	6.1	More Details
CVE-2020-29171	Cross-site scripting (XSS) vulnerability in admin/wp-security-blacklist-menu.php in the Tips and Tricks HQ All In One WP Security & Firewall (all-in-one-wp-security-and-firewall) plugin before 4.4.6 for WordPress.	6.1	More Details
CVE-2020-13565	An open redirect vulnerability exists in the return_page redirection functionality of phpGACL 3.3.7, OpenEMR 5.0.2 and OpenEMR development version 6.0.0 (commit babec93f600ff1394f91ccd512bcad85832eb6ce). A specially crafted HTTP request can redirect users to an arbitrary URL. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35569	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is a self XSS issue with a crafted cookie in the login page.	6.1	More Details
CVE-2021-20644	ELECOM WRC-1467GHBK-A allows arbitrary scripts to be executed on the user's web browser by displaying a specially crafted SSID on the web setup page.	6.1	More Details
CVE-2021-23841	The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).	5.9	More Details
CVE-2021-20409	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 196188.	5.9	More Details
CVE-2021-23336	The package python/cpython from 0 and before 3.6.13, from 3.7.0 and before 3.7.10, from 3.8.0 and before 3.8.8, from 3.9.0 and before 3.9.2 are vulnerable to Web Cache Poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.	5.9	More Details
CVE-2021-20066	JSDom improperly allows the loading of local resources, which allows for local files to be manipulated by a malicious web page when script execution is enabled.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0338	In SystemSettingsValidators, there is a possible permanent denial of service due to missing bounds checks on UI settings. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-156260178	5.5	More Details
CVE-2021-27203	In Dekart Private Disk 2.15, invalid use of the Type3 user buffer for IOCTL codes using METHOD_NEITHER results in arbitrary memory dereferencing.	5.5	More Details
CVE-2021-25688	Under certain conditions, Teradici PCoIP Agents for Windows prior to version 20.10.0 and Teradici PCoIP Agents for Linux prior to version 21.01.0 may log parts of a user's password in the application logs.	5.5	More Details
CVE-2021-20408	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could disclose highly sensitive information to a local user due to inproper storage of a plaintext cryptographic key. IBM X-Force ID: 198187.	5.5	More Details
CVE-2021-27204	Telegram before 7.4 (212543) Stable on macOS stores the local passcode in cleartext, leading to information disclosure.	5.5	More Details
CVE-2020-25340	An issue was discovered in NFStream 5.2.0. Because some allocated modules are not correctly freed, if the nfstream object is directly destroyed without being used after it is created, it will cause a memory leak that may result in a local denial of service (DoS).	5.5	More Details
CVE-2021-27205	Telegram before 7.4 (212543) Stable on macOS stores the local copy of self-destructed messages in a sandbox path, leading to sensitive information disclosure.	5.5	More Details
CVE-2020-35563	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an incomplete XSS filter allowing an attacker to inject crafted malicious code into the page.	5.4	More Details
CVE-2021-26938	A stored XSS issue exists in henriquedornas 5.2.17 via online live chat. NOTE: Third parties report that no such product exists. That henriquedornas is the web design agency and 5.2.17 is simply the PHP version running on this hosts	5.4	More Details
CVE-2021-27231	Hestia Control Panel 1.3.5 and below, in a shared-hosting environment, sometimes allows remote authenticated users to create a subdomain for a different customer's domain name, leading to spoofing of services or email messages.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4954	IBM Spectrum Protect Operations Center 7.1 and 8.1 could allow a remote attacker to bypass authentication restrictions, caused by improper session validation . By using the configuration panel to obtain a valid session using an attacker controlled IBM Spectrum Protect server, an attacker could exploit this vulnerability to bypass authentication and gain access to a limited number of debug functions, such as logging levels. IBM X-Force ID: 192153.	5.4	More Details
CVE-2020-29025	A vulnerability in SiteManager-Embedded (SM-E) Web server which may allow attacker to construct a URL that if visited by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application. This issue affects all versions and variants of SM-E prior to version 9.3	5.4	More Details
CVE-2020-29027	Cross-site Scripting (XSS) vulnerability in GUI of Secomea SiteManager could allow an attacker to cause an XSS Attack. This issue affects: Secomea SiteManager all versions prior to 9.3.	5.4	More Details
CVE-2020-4768	IBM Case Manager 5.2 and 5.3 and IBM Business Automation Workflow 18.0, 19.0, and 20.0 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: 188907.	5.4	More Details
CVE-2021-20654	Wekan, open source kanban board system, between version 3.12 and 4.11, is vulnerable to multiple stored cross-site scripting. This is named 'Fieldbleed' in the vendor's site.	5.4	More Details
CVE-2021-27190	A Stored Cross Site Scripting(XSS) Vulnerability was discovered in PEEL SHOPPING 9.3.0 and 9.4.0, which are publicly available. The user supplied input containing polyglot payload is echoed back in javascript code in HTML response. This allows an attacker to input malicious JavaScript which can steal cookie, redirect them to other malicious website, etc.	5.4	More Details
CVE-2021-20645	Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-22983	On BIG-IP AFM version 15.1.x before 15.1.1, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.5, authenticated users accessing the Configuration utility for AFM are vulnerable to a cross-site scripting attack if they attempt to access a maliciously-crafted URL. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	5.4	More Details
CVE-2021-21022	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to an insecure direct object reference (IDOR) in the product module. Successful exploitation could lead to unauthorized access to restricted resources.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29024	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute vulnerability in (GTA) GoToAppliance of Secomea GateManager could allow an attacker to gain access to sensitive cookies. This issue affects: Secomea GateManager all versions prior to 9.3.	5.3	More Details
CVE-2021-20410	IBM Security Verify Information Queue 1.0.6 and 1.0.7 sends user credentials in plain clear text which can be read by an authenticated user using man in the middle techniques. IBM X-Force ID: 198190.	5.3	More Details
CVE-2021-20407	IBM Security Verify Information Queue 1.0.6 and 1.0.7 discloses sensitive information in source code that could be used in further attacks against the system. IBM X-Force ID: 196185.	5.3	More Details
CVE-2020-35561	An issue was discovered MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual in all versions through v2.11.2. There is an SSRF in the HA module allowing an unauthenticated attacker to scan for open ports.	5.3	More Details
CVE-2020-35566	An issue was discovered in MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual in all versions through v2.11.2. An attacker can read arbitrary JSON files via Local File Inclusion.	5.3	More Details
CVE-2020-35570	An issue was discovered in MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual through 2.11.2. An unauthenticated attacker is able to access files (that should have been restricted) via forceful browsing.	5.3	More Details
CVE-2021-21317	uap-core in an open-source npm package which contains the core of BrowserScope's original user agent string parser. In uap-core before version 0.11.0, some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This is fixed in version 0.11.0. Downstream packages such as uap-python, uap-ruby etc which depend upon uap-core follow different version schemes.	5.3	More Details
CVE-2020-28918	DualShield 5.9.8.0821 allows username enumeration on its login form. A valid username results in prompting for the password, whereas an invalid one will produce an "unknown username" error message.	5.3	More Details
CVE-2021-20404	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user on the network to cause a denial of service due to an invalid cookie value that could prevent future logins. IBM X-Force ID: 196078.	5.3	More Details
CVE-2021-20067	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to view sensitive syslog events without authentication.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29022	Failure to Sanitize host header value on output in the GateManager Web server could allow an attacker to conduct web cache poisoning attacks. This issue affects Secomea GateManager all versions prior to 9.3	5.3	More Details
CVE-2021-21702	In PHP versions 7.3.x below 7.3.27, 7.4.x below 7.4.15 and 8.0.x below 8.0.2, when using SOAP extension to connect to a SOAP server, a malicious SOAP server could return malformed XML data as a response that would cause PHP to access a null pointer and thus cause a crash.	5.3	More Details
CVE-2020-36235	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view custom field and custom SLA names via an Information Disclosure vulnerability in the mobile site view. The affected versions are before version 8.13.2, and from version 8.14.0 before 8.14.1.	5.3	More Details
CVE-2020-28500	Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.	5.3	More Details
CVE-2020-7071	In PHP versions 7.3.x below 7.3.26, 7.4.x below 7.4.14 and 8.0.0, when validating URL with functions like filter_var($url, FILTER_VALIDATE_URL), PHP will accept an URL with invalid password as valid URL. This may lead to functions that rely on URL being valid to mis-parse the URL and produce wrong data as components of the URL.	5.3	More Details
CVE-2020-36237	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view custom field options via an Information Disclosure vulnerability in the /rest/api/2/customFieldOption/ endpoint. The affected versions are before version 8.15.0.	5.3	More Details
CVE-2020-16120	Overlayfs did not properly perform permission checking when copying up files in an overlayfs and could be exploited from within a user namespace, if, for example, unprivileged user namespaces were allowed. It was possible to have a file not readable by an unprivileged user to be copied to a mountpoint controlled by the user, like a removable device. This was introduced in kernel version 4.19 by commit d1d04ef ("ovl: stack file ops"). This was fixed in kernel version 5.8 by commits 56230d9 ("ovl: verify permissions in ovl_path_open()"), 48bd024 ("ovl: switch to mounter creds in readdir") and 05acefb ("ovl: check permission to open real file"). Additionally, commits 130fdbc ("ovl: pass correct flags for opening real directory") and 292f902 ("ovl: call secutiry hook in ovl_real_ioctl()") in kernel 5.8 might also be desired or necessary. These additional commits introduced a regression in overlay mounts within user namespaces which prevented access to files with ownership outside of the user namespace. This regression was mitigated by subsequent commit b6650da ("ovl: do not fail because of O_NOATIMEi") in kernel 5.11.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7021	Elasticsearch versions before 7.10.0 and 6.8.14 have an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens. This could allow an Elasticsearch administrator to view these details.	4.9	More Details
CVE-2020-8355	An internal product security audit of Lenovo XClarity Administrator (LXCA) prior to version 3.1.0 discovered the Windows OS credentials provided by the LXCA user to perform driver updates of managed systems may be captured in the First Failure Data Capture (FFDC) service log if the service log is generated while managed endpoints are updating. The service log is only generated when requested by a privileged LXCA user and it is only accessible to the privileged LXCA user that requested the file and is then deleted.	4.9	More Details
CVE-2021-27233	An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. On the admin portal of the web application, password information for external systems is visible in cleartext. The Settings.asp page is affected by this issue.	4.9	More Details
CVE-2021-27235	An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. On the admin portal of the web application, there is a functionality at diagzip.asp that allows anyone to export tables of a database.	4.9	More Details
CVE-2020-36234	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the Screens Modal view. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.15.0.	4.8	More Details
CVE-2021-21029	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are affected by a Reflected Cross-site Scripting vulnerability via 'file' parameter. Successful exploitation could lead to arbitrary JavaScript execution in the victim's browser. Access to the admin console is required for successful exploitation.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21299	hyper is an open-source HTTP library for Rust (crates.io). In hyper from version 0.12.0 and before versions 0.13.10 and 0.14.3 there is a vulnerability that can enable a request smuggling attack. The HTTP server code had a flaw that incorrectly understands some requests with multiple transfer-encoding headers to have a chunked payload, when it should have been rejected as illegal. This combined with an upstream HTTP proxy that understands the request payload boundary differently can result in "request smuggling" or "desync attacks". To determine if vulnerable, all these things must be true: 1) Using hyper as an HTTP server (the client is not affected), 2) Using HTTP/1.1 (HTTP/2 does not use transfer-encoding), 3) Using a vulnerable HTTP proxy upstream to hyper. If an upstream proxy correctly rejects the illegal transfer-encoding headers, the desync attack cannot succeed. If there is no proxy upstream of hyper, hyper cannot start the desync attack, as the client will repair the headers before forwarding. This is fixed in versions 0.14.3 and 0.13.10. As a workaround one can take the following options: 1) Reject requests that contain a `transfer-encoding` header, 2) Ensure any upstream proxy handles `transfer-encoding` correctly.	4.8	More Details
CVE-2021-27237	The admin panel in BlackCat CMS 1.3.6 allows stored XSS (by an admin) via the Display Name field to backend/preferences/ajax_save.php.	4.8	More Details
CVE-2021-22981	On all versions of BIG-IP 12.1.x and 11.6.x, the original TLS protocol includes a weakness in the master secret negotiation that is mitigated by the Extended Master Secret (EMS) extension defined in RFC 7627. TLS connections that do not use EMS are vulnerable to man-in-the-middle attacks during renegotiation. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	4.8	More Details
CVE-2021-20068	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the error handling functionality of web pages.	4.8	More Details
CVE-2021-23881	A stored cross site scripting vulnerability in ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 February 2021 Update allows an ENS ePO administrator to add a script to a policy event which will trigger the script to be run through a browser block page when a local non-administrator user triggers the policy.	4.8	More Details
CVE-2020-4956	IBM Spectrum Protect Operations Center 7.1 and 8.1 is vulnerable to a denial of service, caused by a RPC that allows certain cache values to be set and dumped to a file. By setting a grossly large cache value and dumping that cached value to a file multiple times, a remote attacker could exploit this vulnerability to cause the consumption of all memory resources. IBM X-Force ID: 192156.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20649	ELECOM WRC-300FEBK-S contains an improper certificate validation vulnerability. Via a man-in-the-middle attack, an attacker may alter the communication response. As a result, an arbitrary OS command may be executed on the affected device.	4.8	More Details
CVE-2021-20070	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the virtualization.php dialogs.	4.8	More Details
CVE-2021-20069	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the regionalSettings.php dialogs.	4.8	More Details
CVE-2021-20071	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the sms.php dialogs.	4.8	More Details
CVE-2021-21060	Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.6	More Details
CVE-2020-29457	A Privilege Elevation vulnerability in OPC UA .NET Standard Stack 1.4.363.107 could allow a rogue application to establish a secure connection.	4.4	More Details
CVE-2020-35568	An issue was discovered in MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual in all versions through v2.11.2. An incomplete filter applied to a database response allows an authenticated attacker to gain non-public information about other users and devices in the account.	4.3	More Details
CVE-2021-21034	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.3	More Details
CVE-2020-35559	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an unused function that allows an authenticated attacker to use up all available IPs of an account and thus not allow creation of new devices and users.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29451	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate Jira projects via an Information Disclosure vulnerability in the Jira Projects plugin report page. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.14.1.	4.3	More Details
CVE-2021-23883	A Null Pointer Dereference vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows a local administrator to cause Windows to crash via a specific system call which is not handled correctly. This varies by machine and had partial protection prior to this update.	4.0	More Details
CVE-2021-23839	OpenSSL 1.0.2 supports SSLv2. If a client attempts to negotiate SSLv2 with a server that is configured to support both SSLv2 and more recent SSL and TLS versions then a check is made for a version rollback attack when unpadding an RSA signature. Clients that support SSL or TLS versions greater than SSLv2 are supposed to use a special form of padding. A server that supports greater than SSLv2 is supposed to reject connection attempts from a client where this special form of padding is present, because this indicates that a version rollback has occurred (i.e. both client and server support greater than SSLv2, and yet this is the version that is being requested). The implementation of this padding check inverted the logic so that the connection attempt is accepted if the padding is present, and rejected if it is absent. This means that such as server will accept a connection if a version rollback attack has occurred. Further the server will erroneously reject a connection if a normal SSLv2 connection attempt is made. Only OpenSSL 1.0.2 servers from version 1.0.2s to 1.0.2x are affected by this issue. In order to be vulnerable a 1.0.2 server must: 1) have configured SSLv2 support at compile time (this is off by default), 2) have configured SSLv2 support at runtime (this is off by default), 3) have configured SSLv2 ciphersuites (these are not in the default ciphersuite list) OpenSSL 1.1.1 does not have SSLv2 support and therefore is not vulnerable to this issue. The underlying error is in the implementation of the RSA_padding_check_SSLv23() function. This also affects the RSA_SSLV23_PADDING padding mode used by various other functions. Although 1.1.1 does not support SSLv2 the RSA_padding_check_SSLv23() function still exists, as does the RSA_SSLV23_PADDING padding mode. Applications that directly call that function or use that padding mode will encounter this issue. However since there is no support for the SSLv2 protocol in 1.1.1 this is considered a bug and not a security issue in that version. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.0.2y (Affected 1.0.2s-1.0.2x).	3.7	More Details
CVE-2020-8030	A Insecure Temporary File vulnerability in skuba of SUSE CaaS Platform 4.5 allows local attackers to leak the bootstrapToken or modify the configuration file before it is processed, leading to arbitrary modifications of the machine/cluster.	3.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29023	Improper Encoding or Escaping of Output from CSV Report Generator of Secomea GateManager allows an authenticated administrator to generate a CSV file that may run arbitrary commands on a victim's computer when opened in a spreadsheet program (like Excel). This issue affects: Secomea GateManager all versions prior to 9.3.	3.5	More Details
CVE-2019-19004	A biWidth*biBitCnt integer overflow in input-bmp.c in autotrace 0.31.1 allows attackers to provide an unexpected input value to malloc via a malformed bitmap image.	3.3	More Details
CVE-2020-10734	A vulnerability was found in keycloak in the way that the OIDC logout endpoint does not have CSRF protection. Versions shipped with Red Hat Fuse 7, Red Hat Single Sign-on 7, and Red Hat Openshift Application Runtimes are believed to be vulnerable.	3.3	More Details
CVE-2020-8029	A Incorrect Permission Assignment for Critical Resource vulnerability in skuba of SUSE CaaS Platform 4.5 allows local attackers to gain access to the kublet key. This issue affects: SUSE CaaS Platform 4.5 skuba versions prior to https://github.com/SUSE/skuba/pull/1416.	2.9	More Details
CVE-2021-20402	IBM Security Verify Information Queue 1.0.6 and 1.0.7 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: 196076.	2.7	More Details
CVE-2021-21296	Fleet is an open source osquery manager. In Fleet before version 3.7.0 a malicious actor with a valid node key can send a badly formatted request that causes the Fleet server to exit, resulting in denial of service. This is possible only while a live query is currently ongoing. We believe the impact of this vulnerability to be low given the requirement that the actor has a valid node key. There is no information disclosure, privilege escalation, or code execution. The issue is fixed in Fleet 3.7.0.	2.7	More Details
CVE-2020-1717	A flaw was found in Keycloak 7.0.1. A logged in user can do an account email enumeration attack.	2.7	More Details
CVE-2021-21301	Wire is an open-source collaboration platform. In Wire for iOS (iPhone and iPad) before version 3.75 there is a vulnerability where the video capture isn't stopped in a scenario where a user first has their camera enabled and then disables it. It's a privacy issue because video is streamed to the call when the user believes it is disabled. It impacts all users in video calls. This is fixed in version 3.75.	2.6	More Details
CVE-2021-22133	The Elastic APM agent for Go versions before 1.11.0 can leak sensitive HTTP header information when logging the details during an application panic. Normally, the APM agent will sanitize sensitive HTTP header details before sending the information to the APM server. During an application panic it is possible the headers will not be sanitized before being sent.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20406	IBM Security Verify Information Queue 1.0.6 and 1.0.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196184.	2.2	More Details
CVE-2021-21063	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Memory corruption vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21059	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Memory corruption vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21062	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Memory corruption vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21049	Adobe Photoshop versions 21.2.4 (and earlier) and 22.1.1 (and earlier) are affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21058	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Memory corruption vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21050	Adobe Photoshop versions 21.2.4 (and earlier) and 22.1.1 (and earlier) are affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21051	Adobe Photoshop versions 21.2.4 (and earlier) and 22.1.1 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted javascript file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21052	Adobe Animate version 21.0.2 (and earlier) is affected by an Out-of-bounds Write vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21048	Adobe Photoshop versions 21.2.4 (and earlier) and 22.1.1 (and earlier) are affected by a Memory Corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	N/A	More Details
CVE-2021-21054	Adobe Illustrator version 25.1 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21027	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are affected by a cross-site request forgery (CSRF) vulnerability via the GraphQL API. Successful exploitation could lead to unauthorized modification of customer metadata by an unauthenticated attacker. Access to the admin console is not required for successful exploitation.	N/A	More Details
CVE-2021-21047	Adobe Photoshop versions 21.2.4 (and earlier) and 22.1.1 (and earlier) are affected by an Out-of-bounds Write vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2020-1973	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-1970	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-1969	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1966	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2021-21061	Acrobat Pro DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2020-35500	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-21046	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21044	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-21015	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to an OS command injection via the customer attribute save controller. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2021-21016	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to OS command injection via the WebAPI. Successful exploitation could lead to remote code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2021-21018	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to OS command injection via the scheduled operation module. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2021-21032	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) do not adequately invalidate user sessions. Successful exploitation of this issue could lead to unauthorized access to restricted resources. Access to the admin console is not required for successful exploitation.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21020	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to an access control bypass vulnerability in the Login as Customer module. Successful exploitation could lead to unauthorized access to restricted resources.	N/A	More Details
CVE-2021-21023	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to a stored cross-site scripting vulnerability in the admin console. Successful exploitation could lead to arbitrary JavaScript execution in the victim's browser. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2021-21024	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are affected by a blind SQL injection vulnerability in the Search module. Successful exploitation could lead to unauthorized access to restricted resources by an unauthenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2021-21031	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) do not adequately invalidate user sessions. Successful exploitation could lead to unauthorized access to restricted resources. Access to the admin console is not required for successful exploitation.	N/A	More Details
CVE-2021-21030	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to a stored cross-site scripting (XSS) in the customer address upload feature. Successful exploitation could lead to arbitrary JavaScript execution in the victim's browser. Exploitation of this issue requires user interaction.	N/A	More Details
CVE-2021-21025	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to XML injection in the product layout updates. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2020-1972	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-1974	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2021-21014	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to a file upload restriction bypass. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35617	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2021-23334	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-3824	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3823	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3822	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3821	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3820	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3819	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2021-21026	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are affected by an improper authorization vulnerability in the integrations module. Successful exploitation could lead to unauthorized access to restricted resources by an unauthenticated attacker. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2020-3817	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3816	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3815	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3814	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3813	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35621	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35620	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35619	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35618	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-3818	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details