SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 July 2020

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-2020-15715	rConfig 3.9.5 could allow a remote authenticated attacker to execute arbitrary code on the system, because of an error in the search.crud.php script. An attacker could exploit this vulnerability using the nodeId parameter.	9.9	More Details
CVE-2020-15860	Parallels Remote Application Server (RAS) 17.1.1 has a Business Logic Error causing remote code execution. It allows an authenticated user to execute any application in the backend operating system through the web application, despite the affected application not being published. In addition, it was discovered that it is possible to access any host in the internal domain, even if it has no published applications or the mentioned host is no longer associated with that server farm.	9.9	More Details
CVE-2019-16244	OMERO.server before 5.6.1 allows attackers to bypass the security filters and access hidden objects via a crafted query.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15420	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-el7-0.9.8.891. Authentication is not required to exploit this vulnerability. The specific flaw exists within loader_ajax.php. When parsing the line 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-9259.	9.8	More Details
CVE-2020-15422	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the archivo 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-9731.	9.8	More Details
CVE-2020-15423	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the dominio 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-9732.	9.8	More Details
CVE-2020-15424	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the domain 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-9735.	9.8	More Details
CVE-2020-15425	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. The issue results from the lack of proper validation of 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-9742.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15426	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_migration_cpanel.php. When parsing the serverip 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-9709.	9.8	More Details
CVE-2020-15427	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_disk_usage.php. When parsing the folderName 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-9713.	9.8	More Details
CVE-2020-15428	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the line 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-9714.	9.8	More Details
CVE-2020-15429	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the user 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-9716.	9.8	More Details
CVE-2020-15430	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the username 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-9736.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15431	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the user 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-9740.	9.8	More Details
CVE-2020-15432	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_migration_cpanel.php. When parsing the filespace 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-9743.	9.8	More Details
CVE-2020-15433	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the phpversion 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-9715.	9.8	More Details
CVE-2020-15434	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the canal 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-9745.	9.8	More Details
CVE-2020-15435	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_start 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-9719.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15606	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. The issue results from the lack of proper validation of 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-9720.	9.8	More Details
CVE-2020-15607	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. When parsing the line 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-9721.	9.8	More Details
CVE-2020-15608	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the ai_service 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-9724.	9.8	More Details
CVE-2020-15609	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_stop 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-9726.	9.8	More Details
CVE-2020-15610	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the modulo 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-9728.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15611	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_restart 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-9734.	9.8	More Details
CVE-2020-15612	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_ftp_manager.php. When parsing the userLogin 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-9737.	9.8	More Details
CVE-2020-15613	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. When parsing the line 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-9739.	9.8	More Details
CVE-2020-15614	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the cha 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-9718.	9.8	More Details
CVE-2020-15615	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_ftp_manager.php. The issue results from the lack of proper validation of 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-9746.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15623	This vulnerability allows remote attackers to write arbitrary files on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the archivo parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9722.	9.8	More Details
CVE-2020-15421	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the check_ip 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-9707.	9.8	More Details
CVE-2020-15900	A memory corruption issue was found in Artifex Ghostscript 9.50 and 9.52. Use of a non-standard PostScript operator can allow overriding of file access controls. The 'rsearch' calculation for the 'post' size resulted in a size that was too large, and could underflow to max uint32_t. This was fixed in commit 5d499272b95a6b890a1397e11d20937de000d31b.	9.8	More Details
CVE-2020-15391	The UI in DevSpace 4.13.0 allows web sites to execute actions on pods (on behalf of a victim) because of a lack of authentication for the WebSocket protocol. This leads to remote code execution.	9.8	More Details
CVE-2020-13919	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	9.8	More Details
CVE-2020-15892	An issue was discovered in apply.cgi on D-Link DAP-1520 devices before 1.10b04Beta02. Whenever a user performs a login action from the web interface, the request values are being forwarded to the ssi binary. On the login page, the web interface restricts the password input field to a fixed length of 15 characters. The problem is that validation is being done on the client side, hence it can be bypassed. When an attacker manages to intercept the login request (POST based) and tampers with the vulnerable parameter (log_pass), to a larger length, the request will be forwarded to the webserver. This results in a stack-based buffer overflow. A few other POST variables, (transferred as part of the login request) are also vulnerable: html_response_page and log_user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15893	An issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet.	9.8	More Details
CVE-2020-9664	Magento versions 1.14.4.5 and earlier, and 1.9.4.5 and earlier have a php object injection vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-4385	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 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: 179266.	9.8	More Details
CVE-2020-10917	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NEC ESMPRO Manager 6.42. Authentication is not required to exploit this vulnerability. The specific flaw exists within the RMI service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10007.	9.8	More Details
CVE-2020-10920	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493.	9.8	More Details
CVE-2020-10921	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482.	9.8	More Details
CVE-2020-15916	goform/AdvSetLanip endpoint on Tenda AC15 AC1900 15.03.05.19 devices allows remote attackers to execute arbitrary system commands via shell metacharacters in the lanIp POST parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15917	common/session.c in Claws Mail before 3.17.6 has a protocol violation because suffix data after STARTTLS is mishandled.	9.8	More Details
CVE-2020-15477	The WebControl in RaspberryTortoise through 2012-10-28 is vulnerable to remote code execution via shell metacharacters in a URI. The file nodejs/raspberryTortoise.js has no validation on the parameter incomingString before passing it to the child_process.exec function.	9.8	More Details
CVE-2020-15492	An issue was discovered in INNEO Startup TOOLS 2017 M021 12.0.66.3784 through 2018 M040 13.0.70.3804. The sut_srv.exe web application (served on TCP port 85) includes user input into a filesystem access without any further validation. This might allow an unauthenticated attacker to read files on the server via Directory Traversal, or possibly have unspecified other impact.	9.8	More Details
CVE-2020-11624	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors.	9.8	More Details
CVE-2020-15920	There is an OS Command Injection in Mida eFramework through 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. No authentication is required.	9.8	More Details
CVE-2020-15921	Mida eFramework through 2.9.0 has a back door that permits a change of the administrative password and access to restricted functionalities, such as Code Execution.	9.8	More Details
CVE-2020-15922	There is an OS Command Injection in Mida eFramework 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. Authentication is required.	9.8	More Details
CVE-2020-12812	An improper authentication vulnerability in SSL VPN in FortiOS 6.4.0, 6.2.0 to 6.2.3, 6.0.9 and below may result in a user being able to log in successfully without being prompted for the second factor of authentication (FortiToken) if they changed the case of their username.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12460	OpenDMARC through 1.3.2 and 1.4.x through 1.4.0-Beta1 has improper null termination in the function opendmarc_xml_parse that can result in a one-byte heap overflow in opendmarc_xml when parsing a specially crafted DMARC aggregate report. This can cause remote memory corruption when a '\0' byte overwrites the heap metadata of the next chunk and its PREV_INUSE flag.	9.8	More Details
CVE-2020-16088	iked in OpenIKED, as used in OpenBSD through 6.7, allows authentication bypass because ca.c has the wrong logic for checking whether a public key matches.	9.8	More Details
CVE-2020-13916	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	9.8	More Details
CVE-2020-13917	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	9.8	More Details
CVE-2020-6522	Inappropriate implementation in external protocol handlers in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-6509	Use after free in extensions in Google Chrome prior to 83.0.4103.116 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2020-6505	Use after free in speech in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-15124	In Goobi Viewer Core before version 4.8.3, a path traversal vulnerability allows for remote attackers to access files on the server via the application. This is limited to files accessible to the application server user, eg. tomcat, but can potentially lead to the disclosure of sensitive information. The vulnerability has been fixed in version 4.8.3	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5377	Dell EMC OpenManage Server Administrator (OMSA) versions 9.4 and prior contain multiple path traversal vulnerabilities. An unauthenticated remote attacker could potentially exploit these vulnerabilities by sending a crafted Web API request containing directory traversal character sequences to gain file system access on the compromised management station.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-6534	Heap buffer overflow in WebRTC in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-5611	Cross-site request forgery (CSRF) vulnerability in Social Sharing Plugin versions prior to 1.2.10 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2020-15714	rConfig 3.9.5 is vulnerable to SQL injection. A remote authenticated attacker could send crafted SQL statements to the devices.crud.php script using the custom_Location parameter, which could allow the attacker to view, add, modify, or delete information in the back-end database.	8.8	More Details
CVE-2020-15713	rConfig 3.9.5 is vulnerable to SQL injection. A remote authenticated attacker could send crafted SQL statements to the devices.php script using the sortBy parameter, which could allow the attacker to view, add, modify, or delete information in the back-end database.	8.8	More Details
CVE-2020-6530	Out of bounds memory access in developer tools in Google Chrome prior to 84.0.4147.89 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2020-15884	A SQL injection vulnerability in TableQuery.php in MunkiReport before 5.6.3 allows attackers to execute arbitrary SQL commands via the order[0][dir] field on POST requests to /datatables/data.	8.8	More Details
CVE-2020-6533	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15901	In Nagios XI before 5.7.3, ajaxhelper.php allows remote authenticated attackers to execute arbitrary commands via cmdsubsys.	8.8	More Details
CVE-2020-15886	A SQL injection vulnerability in reportdata_controller.php in the reportdata module before 3.5 for MunkiReport allows attackers to execute arbitrary SQL commands via the req parameter of the /module/reportdata/ip endpoint.	8.8	More Details
CVE-2020-15887	A SQL injection vulnerability in softwareupdate_controller.php in the Software Update module before 1.6 for MunkiReport allows attackers to execute arbitrary SQL commands via the last URL parameter of the /module/softwareupdate/get_tab_data/ endpoint.	8.8	More Details
CVE-2020-9687	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-9677	Adobe Prelude versions 9.0 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-9685	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-9684	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-8207	Improper access control in Citrix Workspace app for Windows 1912 CU1 and 2006.1 causes privilege escalation and code execution when the automatic updater service is running.	8.8	More Details
CVE-2020-9683	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-15932	Overwolf before 0.149.2.30 mishandles Symbolic Links during updates, causing elevation of privileges.	8.8	More Details
CVE-2020-9680	Adobe Prelude versions 9.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15632	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-842 3.13B05 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of HNAP GetCAPTCHAsetting requests. The issue results from the lack of proper handling of sessions. An attacker can leverage this vulnerability to execute arbitrary code in the context of the device. Was ZDI-CAN-10083.	8.8	More Details
CVE-2020-9678	Adobe Prelude versions 9.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-10923	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPnP service, which listens on TCP port 5000. A crafted UPnP message can be used to bypass authentication. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9642.	8.8	More Details
CVE-2020-10924	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the UPnP service, which listens on TCP port 5000 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9643.	8.8	More Details
CVE-2020-6525	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6524	Heap buffer overflow in WebAudio in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-13970	Shopware before 6.2.3 is vulnerable to a Server-Side Request Forgery (SSRF) in its "Mediabrowser upload by URL" feature. This allows an authenticated user to send HTTP, HTTPS, FTP, and SFTP requests on behalf of the Shopware platform server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15688	The HTTP Digest Authentication in the GoAhead web server before 5.1.2 does not completely protect against replay attacks. This allows an unauthenticated remote attacker to bypass authentication via capture-replay if TLS is not used to protect the underlying communication channel.	8.8	More Details
CVE-2020-10984	Gambio GX before 4.0.1.0 allows admin/admin.php CSRF.	8.8	More Details
CVE-2020-6507	Out of bounds write in V8 in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15416	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9703.	8.8	More Details
CVE-2020-10929	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-9768.	8.8	More Details
CVE-2020-6512	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6513	Heap buffer overflow in PDFium in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15633	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. 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 router. Was ZDI-CAN-10835.	8.8	More Details
CVE-2020-6515	Use after free in tab strip in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-10927	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the encryption of firmware update images. The issue results from the use of an inappropriate encryption algorithm. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9649.	8.8	More Details
CVE-2020-6517	Heap buffer overflow in history in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6518	Use after free in developer tools in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had convinced the user to use developer tools to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-10926	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of firmware updates. The issue results from the lack of proper validation of the firmware image prior to performing an upgrade. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9648.	8.8	More Details
CVE-2020-6520	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10925	This vulnerability allows network-adjacent attackers to compromise the integrity of downloaded information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloading of files via HTTPS. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9647.	8.8	More Details
CVE-2020-6523	Out of bounds write in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-10928	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9767.	8.4	More Details
CVE-2020-12774	D-Link DSL-7740C does not properly validate user input, which allows an authenticated LAN user to inject arbitrary command.	8.2	More Details
CVE-2020-8174	napi_get_value_string_*() allows various kinds of memory corruption in node < 10.21.0, 12.18.0, and < 14.4.0.	8.1	More Details
CVE-2020-15882	A CSRF issue in manager/delete_machine/{id} in MunkiReport before 5.6.3 allows attackers to delete arbitrary machines from the MunkiReport database.	8.1	More Details
CVE-2020-15631	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 1.04B03_HOTFIX WiFi extenders. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the HNAP service, which listens on TCP port 80 by default. When parsing the SOAPAction 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-10084.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7514	A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker access to the authorization credentials for a device and gain full access.	7.8	More Details
CVE-2020-7515	A CWE-321: Use of hard-coded cryptographic key stored in cleartext vulnerability exists in Easergy Builder V1.4.7.2 and prior which could allow an attacker to decrypt a password.	7.8	More Details
CVE-2020-7516	A CWE-316: Cleartext Storage of Sensitive Information in Memory vulnerability exists in Easergy Builder V1.4.7.2 and prior which could allow an attacker access to login credentials.	7.8	More Details
CVE-2020-10606	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment.	7.8	More Details
CVE-2020-10608	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification.	7.8	More Details
CVE-2020-10610	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification.	7.8	More Details
CVE-2020-15593	SteelCentral Aternity Agent 11.0.0.120 on Windows mishandles IPC. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. Any user in the system is allowed to access the interprocess communication channel AternityAgentAssistantIpc, retrieve a serialized object and call object methods remotely. Among others, the methods allow any user to: (1) Create and/or overwrite arbitrary XML files across the system; (2) Create arbitrary directories across the system; and (3) Load arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)/Aternity Information Systems/Assistant/plugins" directory and execute code contained in them.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1425	A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1457.	7.8	More Details
CVE-2020-1457	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1425.	7.8	More Details
CVE-2020-11474	NCP Secure Enterprise Client before 10.15 r47589 allows a symbolic link attack on enumusb.reg via Support Assistant.	7.8	More Details
CVE-2020-15904	A buffer overflow in the patching routine of bsdiff4 before 1.2.0 allows an attacker to write to heap memory (beyond allocated bounds) via a crafted patch file.	7.8	More Details
CVE-2020-15778	scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."	7.8	More Details
CVE-2020-4372	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 179009	7.8	More Details
CVE-2020-6510	Heap buffer overflow in background fetch in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	7.8	More Details
CVE-2019-18619	Incorrect parameter validation in the synaTee component of Synaptics WBF drivers using an SGX enclave (all versions prior to 2019-11-15) allows a local user to execute arbitrary code in the enclave (that can compromise confidentiality of enclave data) via APIs that accept invalid pointers.	7.8	More Details
CVE-2020-9674	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9676	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9675	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-15622	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the search parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9712.	7.5	More Details
CVE-2020-15619	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the type parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9723.	7.5	More Details
CVE-2020-15620	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the id parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9741.	7.5	More Details
CVE-2020-15621	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the email parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9711.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15896	An authentication-bypass issue was discovered on D-Link DAP-1522 devices 1.4x before 1.10b04Beta02. There exist a few pages that are directly accessible by any unauthorized user, e.g., logout.php and login.php. This occurs because of checking the value of NO_NEED_AUTH. If the value of NO_NEED_AUTH is 1, the user has direct access to the webpage without any authentication. By appending a query string NO_NEED_AUTH with the value of 1 to any protected URL, any unauthorized user can access the application directly, as demonstrated by bsc_lan.php?NO_NEED_AUTH=1.	7.5	More Details
CVE-2020-6098	An exploitable denial of service vulnerability exists in the freeDiameter functionality of freeDiameter 1.3.2. A specially crafted Diameter request can trigger a memory corruption resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2020-15806	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation.	7.5	More Details
CVE-2020-3452	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.	7.5	More Details
CVE-2020-15624	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_new_account.php. When parsing the domain parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9727.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15625	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_add_mailbox.php. When parsing the username parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9729.	7.5	More Details
CVE-2020-15626	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the term parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9730.	7.5	More Details
CVE-2020-15627	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the account parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9738.	7.5	More Details
CVE-2020-15894	An issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. There exists an exposed administration function in getcfg.php, which can be used to call various services. It can be utilized by an attacker to retrieve various sensitive information, such as admin login credentials, by setting the value of _POST_SERVICES in the query string to DEVICE.ACCOUNT.	7.5	More Details
CVE-2020-10604	In OSIsoft PI System multiple products and versions, a remote, unauthenticated attacker could crash PI Network Manager service through specially crafted requests. This can result in blocking connections and queries to PI Data Archive.	7.5	More Details
CVE-2020-15923	Mida eFramework through 2.9.0 allows unauthenticated ../ directory traversal.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15618	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the username parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9717.	7.5	More Details
CVE-2020-7681	This affects all versions of package marscode. There is no path sanitization in the path provided at fs.readFile in index.js.	7.5	More Details
CVE-2020-7682	This affects all versions of package marked-tree. There is no path sanitization in the path provided at fs.readFile in index.js.	7.5	More Details
CVE-2020-7683	This affects all versions of package rollup-plugin-server. There is no path sanitization in readFile operation performed inside the readFileFromContentBase function.	7.5	More Details
CVE-2020-7686	This affects all versions of package rollup-plugin-dev-server. There is no path sanitization in readFile operation inside the readFileFromContentBase function.	7.5	More Details
CVE-2020-7687	This affects all versions of package fast-http. There is no path sanitization in the path provided at fs.readFile in index.js.	7.5	More Details
CVE-2020-15617	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the status parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9708.	7.5	More Details
CVE-2020-15616	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the package parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9706.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13918	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	7.5	More Details
CVE-2020-13915	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	7.5	More Details
CVE-2020-13914	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	7.5	More Details
CVE-2020-15592	SteelCentral Aternity Agent before 11.0.0.120 on Windows allows Privilege Escalation via a crafted file. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. The remotely callable methods from remotable objects available through interprocess communication allow loading of arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)%/Aternity Information Systems/Assistant/plugins" directory, where the name of the plugin is passed as part of an XML-serialized object. However, because the name of the DLL is concatenated with the ".\plugins" string, a directory traversal vulnerability exists in the way plugins are resolved.	7.5	More Details
CVE-2020-4375	IBM MQ, IBM MQ Appliance, IBM MQ for HPE NonStop 8.0, 9.1 CD, and 9.1 LTS could allow an attacker to cause a denial of service due to a memory leak caused by an error creating a dynamic queue. IBM X-Force ID: 179080.	7.5	More Details
CVE-2020-12845	Cherokee 0.4.27 to 1.2.104 is affected by a denial of service due to a NULL pointer dereferences. A remote unauthenticated attacker can crash the server by sending an HTTP request to protected resources using a malformed Authorization header that is mishandled during a cherokee_buffer_add call within cherokee_validator_parse_basic or cherokee_validator_parse_digest.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15924	There is a SQL Injection in Mida eFramework through 2.9.0 that leads to Information Disclosure. No authentication is required. The injection point resides in one of the authentication parameters.	7.5	More Details
CVE-2020-15628	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the user parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9710.	7.5	More Details
CVE-2020-15419	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Veeam ONE 10.0.0.750_20200415. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Reporter_ImportLicense class. Due to the improper restriction of XML External Entity (XXE) references, a specially crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose file contents in the context of SYSTEM. Was ZDI-CAN-10710.	7.5	More Details
CVE-2020-7491	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4.	7.5	More Details
CVE-2020-4400	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 179478.	7.5	More Details
CVE-2020-15908	tar/TarFileReader.cpp in Cauldron cbang (aka C-Bang or C!) before 1.6.0 allows Directory Traversal during extraction from a TAR archive.	7.5	More Details
CVE-2020-11440	httpRpmFs in WebCLI in Wind River VxWorks 5.5 through 7 SR0640 has no check for an escape from the web root.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13997	In Shopware before 6.2.3, the database password is leaked to an unauthenticated user when a DriverException occurs and verbose error handling is enabled.	7.5	More Details
CVE-2020-16094	In imap_scan_tree_recursive in Claws Mail through 3.17.6, a malicious IMAP server can trigger stack consumption because of unlimited recursion into subdirectories during a rebuild of the folder tree.	7.5	More Details
CVE-2020-15899	Grin 3.0.0 before 4.0.0 has insufficient validation of data related to Mimblewimble.	7.5	More Details
CVE-2020-10918	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182.	7.5	More Details
CVE-2020-10922	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527.	7.5	More Details
CVE-2020-15418	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Veeam ONE 10.0.0.750_20200415. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSRSReport class. Due to the improper restriction of XML External Entity (XXE) references, a specially crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose file contents in the context of SYSTEM. Was ZDI-CAN-10709.	7.5	More Details
CVE-2020-10609	Grundfos CIM 500 v06.16.00 stores plaintext credentials, which may allow sensitive information to be read or allow modification to system settings by someone with access to the device.	7.5	More Details
CVE-2020-7518	A CWE-20: Improper input validation vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to modify project configuration files.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7519	A CWE-521: Weak Password Requirements vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to compromise a user account.	7.5	More Details
CVE-2020-15953	LibEtPan through 1.9.4, as used in MailCore 2 through 0.6.3 and other products, has a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a meddler-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection."	7.4	More Details
CVE-2020-8317	A DLL search path vulnerability was reported in Lenovo Drivers Management prior to version 2.7.1128.1046 that could allow an authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2020-8326	An unquoted service path vulnerability was reported in Lenovo Drivers Management prior to version 2.7.1128.1046 that could allow an authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2020-11476	Concrete5 before 8.5.3 allows Unrestricted Upload of File with Dangerous Type such as a .phar file.	7.2	More Details
CVE-2020-11623	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. An attacker with physical access to the UART interface could access additional diagnostic and configuration functionalities as well as the camera's bootloader. Successful exploitation could compromise confidentiality, integrity, and availability of the affected system. It could even render the device inoperable.	6.8	More Details
CVE-2020-12638	An encryption-bypass issue was discovered on Espressif ESP-IDF devices through 4.2, ESP8266_NONOS_SDK devices through 3.0.3, and ESP8266_RTOS_SDK devices through 3.3. Broadcasting forged beacon frames forces a device to change its authentication mode to OPEN, effectively disabling its 802.11 encryption.	6.8	More Details
CVE-2020-7017	In Kibana versions before 6.8.11 and 7.8.1 the region map visualization in contains a stored XSS flaw. An attacker who is able to edit or create a region map visualization could obtain sensitive information or perform destructive actions on behalf of Kibana users who view the region map visualization.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14297	A flaw was discovered in Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and cause denial of service attack and make services unavailable.	6.5	More Details
CVE-2020-15126	In parser-server from version 3.5.0 and before 4.3.0, an authenticated user using the viewer GraphQL query can by pass all read security on his User object and can also by pass all objects linked via relation or Pointer on his User object.	6.5	More Details
CVE-2020-6511	Information leak in content security policy in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-4399	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 could allow an authenticated user to send malformed requests to cause a denial of service against the server. IBM X-Force ID: 179476.	6.5	More Details
CVE-2020-4465	IBM MQ, IBM MQ Appliance, and IBM MQ for HPE NonStop 8.0, 9.1 CD, and 9.1 LTS is vulnerable to a buffer overflow vulnerability due to an error within the channel processing code. A remote attacker could overflow the buffer using an older client and cause a denial of service. IBM X-Force ID: 181562.	6.5	More Details
CVE-2020-6519	Policy bypass in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.	6.5	More Details
CVE-2020-10643	An authenticated remote attacker could use specially crafted URLs to send a victim using PI Vision 2019 mobile to a vulnerable web page due to a known issue in a third-party component.	6.5	More Details
CVE-2020-14307	A vulnerability was found in Wildfly's Enterprise Java Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable.	6.5	More Details
CVE-2020-15954	KDE KMail 19.12.3 (aka 5.13.3) engages in unencrypted POP3 communication during times when the UI indicates that encryption is in use.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6506	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 83.0.4103.106 allowed a remote attacker to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2020-9679	Adobe Prelude versions 9.0 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution.	6.5	More Details
CVE-2020-15912	Tesla Model 3 vehicles allow attackers to open a door by leveraging access to a legitimate key card, and then using NFC Relay. NOTE: the vendor has developed Pin2Drive to mitigate this issue	6.5	More Details
CVE-2020-6521	Side-channel information leakage in autofill in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2020-6514	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream.	6.5	More Details
CVE-2020-10930	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of URLs. The issue results from the lack of proper routing of URLs. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-9618.	6.5	More Details
CVE-2020-9686	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution.	6.5	More Details
CVE-2020-6526	Inappropriate implementation in iframe sandbox in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-8559	The Kubernetes kube-apiserver in versions v1.6-v1.15, and versions prior to v1.16.13, v1.17.9 and v1.18.6 are vulnerable to an unvalidated redirect on proxied upgrade requests that could allow an attacker to escalate privileges from a node compromise to a full cluster compromise.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15417	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. A crafted gui_region in a string table file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9756.	6.3	More Details
CVE-2020-13913	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	6.1	More Details
CVE-2020-6535	Insufficient data validation in WebUI in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page.	6.1	More Details
CVE-2020-15902	Graph Explorer in Nagios XI before 5.7.2 allows XSS via the link url option.	6.1	More Details
CVE-2020-9665	Magento versions 1.14.4.5 and earlier, and 1.9.4.5 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	6.1	More Details
CVE-2020-15881	A Cross-Site Scripting (XSS) vulnerability in the munki_facts (aka Munki Conditions) module before 1.5 for MunkiReport allows remote attackers to inject arbitrary web script or HTML via the key name.	6.1	More Details
CVE-2020-15919	A Reflected Cross Site Scripting (XSS) vulnerability was discovered in Mida eFramework through 2.9.0.	6.1	More Details
CVE-2020-15895	An XSS issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. In the file webinc/js/info.php, no output filtration is applied to the RESULT parameter, before it's printed on the webpage.	6.1	More Details
CVE-2019-18834	Persistent XSS in the WooCommerce Subscriptions plugin before 2.6.3 for WordPress allows remote attackers to execute arbitrary JavaScript because Billing Details are mishandled in WCS_Admin_Post_Types in class-wcs-admin-post-types.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15883	A Cross-Site Scripting (XSS) vulnerability in the managedinstalls module before 2.6 for MunkiReport allows remote attackers to inject arbitrary web script or HTML via the last two URL parameters (through which installed packages names and versions are reported).	6.1	More Details
CVE-2019-18618	Incorrect access control in the firmware of Synaptics VFS75xx family fingerprint sensors that include external flash (all versions prior to 2019-11-15) allows a local administrator or physical attacker to compromise the confidentiality of sensor data via injection of an unverified partition table.	6.0	More Details
CVE-2020-4397	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 transmits sensitive information in plain text which could be obtained by an attacker using man in the middle techniques. IBM X-Force ID: 179428.	5.9	More Details
CVE-2020-10600	An authenticated remote attacker could crash PI Archive Subsystem when the subsystem is working under memory pressure. This can result in blocking queries to PI Data Archive (2018 SP2 and prior versions).	5.9	More Details
CVE-2020-10919	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185.	5.9	More Details
CVE-2019-11252	The Kubernetes kube-controller-manager in versions v1.0-v1.17 is vulnerable to a credential leakage via error messages in mount failure logs and events for AzureFile and CephFS volumes.	5.9	More Details
CVE-2020-4369	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 stores highly sensitive information in cleartext that could be obtained by a user. IBM X-Force ID: 179004.	5.5	More Details
CVE-2020-8175	Uncontrolled resource consumption in `jpeg-js` before 0.4.0 may allow attacker to launch denial of service attacks using specially a crafted JPEG image.	5.5	More Details
CVE-2020-8557	The Kubernetes kubelet component in versions 1.1-1.16.12, 1.17.0-1.17.8 and 1.18.0-1.18.5 do not account for disk usage by a pod which writes to its own /etc/hosts file. The /etc/hosts file mounted in a pod by kubelet is not included by the kubelet eviction manager when calculating ephemeral storage usage by a pod. If a pod writes a large amount of data to the /etc/hosts file, it could fill the storage space of the node and cause the node to fail.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7517	A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to read user credentials.	5.5	More Details
CVE-2020-15945	Lua through 5.4.0 has a segmentation fault in changedline in ldebug.c (e.g., when called by luaG_traceexec) because it incorrectly expects that an oldpc value is always updated upon a return of the flow of control to a function.	5.5	More Details
CVE-2019-4731	IBM MQ Appliance 9.1.4.CD could allow a local attacker to obtain highly sensitive information by inclusion of sensitive data within trace. IBM X-Force ID: 172616.	5.5	More Details
CVE-2020-12880	An issue was discovered in Pulse Policy Secure (PPS) and Pulse Connect Secure (PCS) Virtual Appliance before 9.1R8. By manipulating a certain kernel boot parameter, it can be tricked into dropping into a root shell in a pre-install phase where the entire source code of the appliance is available and can be retrieved. (The source code is otherwise inaccessible because the appliance has its hard disks encrypted, and no root shell is available during normal operation.)	5.5	More Details
CVE-2020-11110	Grafana through 6.7.1 allows stored XSS due to insufficient input protection in the originalUrl field, which allows an attacker to inject JavaScript code that will be executed after clicking on Open Original Dashboard after visiting the snapshot.	5.4	More Details
CVE-2020-15918	Multiple Stored Cross Site Scripting (XSS) vulnerabilities were discovered in Mida eFramework through 2.9.0.	5.4	More Details
CVE-2020-4447	IBM FileNet Content Manager 5.5.3 and 5.5.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 181227.	5.4	More Details
CVE-2020-8558	The Kubelet and kube-proxy components in versions 1.1.0-1.16.10, 1.17.0-1.17.6, and 1.18.0-1.18.3 were found to contain a security issue which allows adjacent hosts to reach TCP and UDP services bound to 127.0.0.1 running on the node or in the node's network namespace. Such a service is generally thought to be reachable only by other processes on the same host, but due to this defeect, could be reachable by other hosts on the same LAN as the node, or by containers running on the same node as the service.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15885	A Cross-Site Scripting (XSS) vulnerability in the comment module before 4.0 for MunkiReport allows remote attackers to inject arbitrary web script or HTML by posting a new comment.	5.4	More Details
CVE-2020-4318	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics 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: 177356.	5.4	More Details
CVE-2020-4317	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics 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: 177355.	5.4	More Details
CVE-2020-7685	This affects all versions of package UmbracoForms. When using the default configuration for upload forms, it is possible to upload arbitrary file types. The package offers a way for users to mitigate the issue. The users of this package can create a custom workflow and frontend validation that blocks certain file types, depending on their security needs and policies.	5.4	More Details
CVE-2020-14175	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in user macro parameters. The affected versions are before version 7.4.2, and from version 7.5.0 before 7.5.2.	5.4	More Details
CVE-2020-13971	In Shopware before 6.2.3, authenticated users are allowed to use the Mediabrowser fileupload feature to upload SVG images containing JavaScript. This leads to Persistent XSS. An uploaded image can be accessed without authentication.	5.4	More Details
CVE-2020-9663	Adobe Reader Mobile versions 20.0.1 and earlier have a directory traversal vulnerability. Successful exploitation could lead to information disclosure.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11625	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. Failed web UI login attempts elicit different responses depending on whether a user account exists. Because the responses indicate whether a submitted username is valid or not, they make it easier to identify legitimate usernames. If a login request is sent to ISAPI/Security/sessionLogin/capabilities using a username that exists, it will return the value of the salt given to that username, even if the password is incorrect. However, if a login request is sent using a username that is not present in the database, it will return an empty salt value. This allows attackers to enumerate legitimate usernames, facilitating brute-force attacks. NOTE: this is different from CVE-2020-7057.	5.3	More Details
CVE-2020-7695	Uvicorn before 0.11.7 is vulnerable to HTTP response splitting. CRLF sequences are not escaped in the value of HTTP headers. Attackers can exploit this to add arbitrary headers to HTTP responses, or even return an arbitrary response body, whenever crafted input is used to construct HTTP headers.	5.3	More Details
CVE-2020-10602	In OSIsoft PI System multiple products and versions, an authenticated remote attacker could crash PI Network Manager due to a race condition. This can result in blocking connections and queries to PI Data Archive.	5.3	More Details
CVE-2020-15863	hw/net/xgmac.c in the XGMAC Ethernet controller in QEMU before 07-20-2020 has a buffer overflow. This occurs during packet transmission and affects the highbank and midway emulated machines. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service or potential privileged code execution. This was fixed in commit 5519724a13664b43e225ca05351c60b4468e4555.	5.3	More Details
CVE-2014-1422	In Ubuntu's trust-store, if a user revokes location access from an application, the location is still available to the application because the application will honour incorrect, cached permissions. This is because the cache was not ordered by creation time by the Select struct in src/core/trust/impl/sqlite3/store.cpp. Fixed in trust-store (Ubuntu) version 1.1.0+15.04.20150123-0ubuntu1 and trust-store (Ubuntu RTM) version 1.1.0+15.04.20150123~rtm-0ubuntu1.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14725	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-15120	In "I hate money" before version 4.1.5, an authenticated member of one project can modify and delete members of another project, without knowledge of this other project's private code. This can be further exploited to access all bills of another project without knowledge of this other project's private code. With the default configuration, anybody is allowed to create a new project. An attacker can create a new project and then use it to become authenticated and exploit this flaw. As such, the exposure is similar to an unauthenticated attack, because it is trivial to become authenticated. This is fixed in version 4.1.5.	4.9	More Details
CVE-2020-10983	Gambio GX before 4.0.1.0 allows SQL Injection in admin/mobile.php.	4.9	More Details
CVE-2020-10982	Gambio GX before 4.0.1.0 allows SQL Injection in admin/gv_mail.php.	4.9	More Details
CVE-2020-10985	Gambio GX before 4.0.1.0 allows XSS in admin/coupon_admin.php.	4.8	More Details
CVE-2020-7016	Kibana versions before 6.8.11 and 7.8.1 contain a denial of service (DoS) flaw in Timelion. An attacker can construct a URL that when viewed by a Kibana user can lead to the Kibana process consuming large amounts of CPU and becoming unresponsive.	4.8	More Details
CVE-2020-10614	In OSIsoft PI System multiple products and versions, an authenticated remote attacker with write access to PI Vision databases could inject code into a display. Unauthorized information disclosure, deletion, or modification is possible if a victim views the infected display.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7520	A CWE-601: URL Redirection to Untrusted Site ('Open Redirect') vulnerability exists in Schneider Electric Software Update (SESU), V2.4.0 and prior, which could cause execution of malicious code on the victim's machine. In order to exploit this vulnerability, an attacker requires privileged access on the engineering workstation to modify a Windows registry key which would divert all traffic updates to go through a server in the attacker's possession. A man-in-the-middle attack is then used to complete the exploit.	4.7	More Details
CVE-2020-4408	The IBM QRadar Advisor 1.1 through 2.5.2 with Watson App for IBM QRadar SIEM does not adequately mask all passwords during input, which could be obtained by a physical attacker nearby. IBM X-Force ID: 179536.	4.6	More Details
CVE-2020-4498	IBM MQ Appliance 9.1 LTS and 9.1 CD could allow a local privileged user to obtain highly sensitve information due to inclusion of data within trace files. IBM X-Force ID: 182118.	4.4	More Details
CVE-2020-6516	Policy bypass in CORS in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2020-6531	Side-channel information leakage in scroll to text in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2020-4319	IBM MQ, IBM MQ Appliance, and IBM MQ for HPE NonStop 8.0, 9.1 LTS, and 9.1 CD could allow under special circumstances, an authenticated user to obtain sensitive information due to a data leak from an error message within the pre-v7 pubsub logic. IBM X-Force ID: 177402.	4.3	More Details
CVE-2020-4405	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 could disclose potentially sensitive information to an authenticated user due to world readable log files. IBM X-Force ID: 179484.	4.3	More Details
CVE-2020-15712	rConfig 3.9.5 could allow a remote authenticated attacker to traverse directories on the system. An attacker could send a crafted request to the ajaxGetFileByPath.php script containing hexadecimal encoded "dot dot" sequences (%2f..%2f) in the path parameter to view arbitrary files on the system.	4.3	More Details
CVE-2020-6529	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to leak cross-origin data via a crafted HTML page.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6528	Incorrect security UI in basic auth in Google Chrome on iOS prior to 84.0.4147.89 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2020-6536	Incorrect security UI in PWAs in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had persuaded the user to install a PWA to spoof the contents of the Omnibox (URL bar) via a crafted PWA.	4.3	More Details
CVE-2020-6527	Insufficient policy enforcement in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.	4.3	More Details
CVE-2020-15408	An issue was discovered in Pulse Secure Pulse Connect Secure before 9.1R8. An authenticated attacker can access the admin page console via the end-user web interface because of a rewrite.	3.7	More Details
CVE-2020-7694	This affects all versions of package uvicorn. The request logger provided by the package is vulnerable to ASNI escape sequence injection. Whenever any HTTP request is received, the default behaviour of uvicorn is to log its details to either the console or a log file. When attackers request crafted URLs with percent-encoded escape sequences, the logging component will log the URL after it's been processed with urllib.parse.unquote, therefore converting any percent-encoded characters into their single-character equivalent, which can have special meaning in terminal emulators. By requesting URLs with crafted paths, attackers can: * Pollute uvicorn's access logs, therefore jeopardising the integrity of such files. * Use ANSI sequence codes to attempt to interact with the terminal emulator that's displaying the logs (either in real time or from a file).	3.7	More Details
CVE-2020-15103	In FreeRDP less than or equal to 2.1.2, an integer overflow exists due to missing input sanitation in rdpegfx channel. All FreeRDP clients are affected. The input rectangles from the server are not checked against local surface coordinates and blindly accepted. A malicious server can send data that will crash the client later on (invalid length arguments to a `memcpy`) This has been fixed in 2.2.0. As a workaround, stop using command line arguments /gfx, /gfx-h264 and /network:auto	3.5	More Details
CVE-2020-4371	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 contains sensitive information in leftover debug code that could be used aid a local user in further attacks against the system. IBM X-Force ID: 179008.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9077	HUAWEI P30 smart phones with versions earlier than 10.1.0.160(C00E160R2P11) have an information exposure vulnerability. The system does not properly authenticate the application that access a specified interface. Attackers can trick users into installing malicious software to exploit this vulnerability and obtain some information about the device. Successful exploit may cause information disclosure.	3.3	More Details
CVE-2020-9251	HUAWEI Mate 20 smartphones with versions earlier than 10.1.0.160(C00E160R2P11) have an improper authorization vulnerability. The software does not properly restrict certain operation in certain scenario, the attacker should do certain configuration before the user turns on student mode function. Successful exploit could allow the attacker to bypass the limit of student mode function. Affected product versions include: HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8).	2.4	More Details