Vulnerability Summary for the Week of February 8, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	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.	2021-02-11	9.3	CVE-2021-21044 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	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.	2021-02-11	9.3	CVE-2021-21045 MISC
advantech -- iview	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'.	2021-02-11	7.5	CVE-2021-22658 MISC MISC
asus -- rt-ax3000_firmware	Denial of service in ASUSWRT ASUS RT-AX3000 firmware versions 3.0.0.4.384_10177 and earlier versions allows an attacker to disrupt the use of device setup services via continuous login error.	2021-02-05	7.8	CVE-2021-3229 MISC MISC MISC
carrierwave_project -- carrierwave	CarrierWave is an open-source RubyGem which provides a simple and flexible way to upload files from Ruby applications. In	2021-02-08	7.5	CVE-2021-21305

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CarrierWave before versions 1.3.2 and 2.1.1, there is a code injection vulnerability. The "#manipulate!" method inappropriately evals the content of mutation option(:read/:write), allowing attackers to craft a string that can be executed as a Ruby code. If an application developer supplies untrusted inputs to the option, it will lead to remote code execution(RCE). This is fixed in versions 1.3.2 and 2.1.1.			MISC MISC MISC CONFIRM MISC
college_management_system_project -- college_management_system	College Management System Php 1.0 suffers from SQL injection vulnerabilities in the index.php page from POST parameters 'unametxt' and 'pwdtxt', which are not filtered before passing a SQL query.	2021-02-08	7.5	CVE-2020-26051 MISC
dell -- emc_powerscale_onefs	Dell PowerScale OneFS versions 8.1.0 – 9.1.0 contain a "use of SSH key past account expiration" vulnerability. A user on the network with the ISI_PRIV_AUTH_SSH RBAC privilege that has an expired account may potentially exploit this vulnerability, giving them access to the same things they had before	2021-02-09	7.5	CVE-2021-21502 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	account expiration. This may by a high privileged account and hence Dell recommends customers upgrade at the earliest opportunity.			
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.1.0 - 9.1.0 contain an improper input validation vulnerability. A user with the ISI_PRIV_CLUSTER privilege may exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	2021-02-09	7.2	CVE-2020-26193 MISC
dynamoosejs -- dynamoose	Dynamoose is an open-source modeling tool for Amazon's DynamoDB. In Dynamoose from version 2.0.0 and before version 2.7.0 there was a prototype pollution vulnerability in the internal utility method "lib/utils/object/set.ts". This method is used throughout the codebase for various operations throughout Dynamoose. We have not seen any evidence of this vulnerability being exploited. There is no evidence this vulnerability impacts versions 1.x.x since the vulnerable method was added as part of	2021-02-08	7.5	CVE-2021-21304 MISC MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the v2 rewrite. This vulnerability also impacts v2.x.x beta/alpha versions. Version 2.7.0 includes a patch for this vulnerability.			
elecom -- wrc-300febk-s_firmware	ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.	2021-02-12	7.7	CVE-2021-20648 MISC MISC
epikur -- epikur	An issue was discovered in Epikur before 20.1.1. The Epikur server contains the checkPasswort() function that, upon user login, checks the submitted password against the user password's MD5 hash stored in the database. It is also compared to a second MD5 hash, which is the same for every user (aka a "Backdoor Password" of 3p1kursupport). If the submitted password matches either one, access is granted.	2021-02-05	7.5	CVE-2020-10539 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The	2021-02-10	7.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	web daemon contains the hardcoded admin / lnadmin credentials for an ISP.			27145 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / admin credentials for an ISP.	2021-02-10	7.5	CVE-2021-27147 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded telecomadmin / nE7jA%5m credentials for an ISP.	2021-02-10	7.5	CVE-2021-27148 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded adminpldt / z6dUABtl270qRxt7a2uGTiw credentials for an ISP.	2021-02-10	7.5	CVE-2021-27149 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / CUadmin credentials for an ISP.	2021-02-10	7.5	CVE-2021-27146 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded rootmet / m3tr0r00t credentials for an ISP.	2021-02-10	7.5	CVE-2021-27151 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded awnfibre / fibre@dm!n credentials for an ISP.	2021-02-10	7.5	CVE-2021-27152 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded trueadmin / admintrue credentials for an ISP.	2021-02-10	7.5	CVE-2021-27153 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / G0R2U1P2ag credentials for an ISP.	2021-02-10	7.5	CVE-2021-27154 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin	2021-02-10	7.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/ 3UJUh2VemEfUtesEchEC2d2e credentials for an ISP.			27155 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	7.5	CVE-2021-27156 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 888888 credentials for an ISP.	2021-02-10	7.5	CVE-2021-27157 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded L1vt1m4eng / 888888 credentials for an ISP.	2021-02-10	7.5	CVE-2021-27158 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded useradmin / 888888 credentials for an ISP.	2021-02-10	7.5	CVE-2021-27159 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / 888888 credentials for an ISP.	2021-02-10	7.5	CVE-2021-27160 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 1234 credentials for an ISP.	2021-02-10	7.5	CVE-2021-27161 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / tattoo@home credentials for an ISP.	2021-02-10	7.5	CVE-2021-27162 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / tele1234 credentials for an ISP.	2021-02-10	7.5	CVE-2021-27163 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded gestiontelebucaramanga /	2021-02-10	7.5	CVE-2021-27150 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	t3l3buc4r4m4ng42013 credentials for an ISP.			
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / aisadmin credentials for an ISP.	2021-02-10	7.5	CVE-2021-27164 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	7.5	CVE-2021-27177 MISC
fiberhome -- hg6245d_firmware	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).	2021-02-10	10	CVE-2021-27171 MISC
fortinet -- fortiisolator	An insufficient session expiration vulnerability in FortiNet's FortiIsolator version 2.0.1 and below may allow an attacker to reuse the unexpired admin user	2021-02-08	7.5	CVE-2020-6649 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	session IDs to gain admin privileges, should the attacker be able to obtain that session ID (via other, hypothetical attacks)			
genivia -- gsoap	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.	2021-02-10	7.5	CVE-2020-13576 MISC
gitlog_project -- gitlog	The gitlog function in src/index.ts in gitlog before 4.0.4 has a command injection vulnerability.	2021-02-08	7.5	CVE-2021-26541 MISC MISC
google -- android	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:	2021-02-10	10	CVE-2021-0326 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android-10 Android-11 Android-8.1 Android-9Android ID: A-172937525			
google -- android	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	2021-02-10	9.3	CVE-2021-0302 MISC
google -- android	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	2021-02-10	9.3	CVE-2021-0305 MISC
google -- android	In ih264d_parse_pslice of ih264d_parse_pslice.c, there is a possible out of bounds write due to a heap buffer	2021-02-10	9.3	CVE-2021-0325 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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			
google -- android	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	2021-02-10	7.2	CVE-2021-0334 MISC
google -- android	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	2021-02-10	9.3	CVE-2021-0340 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-10Android ID: A-134155286			
google -- android	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	2021-02-10	9.3	CVE-2021-0339 MISC
google -- android	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	2021-02-10	7.2	CVE-2021-0332 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	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	2021-02-10	7.2	CVE-2021-0336 MISC
google -- android	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	2021-02-10	7.2	CVE-2021-0330 MISC
google -- android	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	2021-02-10	7.2	CVE-2021-0328 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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			
google -- android	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	2021-02-10	7.2	CVE-2021-0329 MISC
google -- android	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	2021-02-10	7.2	CVE-2021-0337 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Android-10 Android-11Android ID: A-157474195			
google -- android	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	2021-02-10	7.2	CVE-2021-0327 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webstartflash function.	2021-02-08	7.2	CVE-2021-25142 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetlicensecfg function.	2021-02-08	7.2	CVE-2021-25171 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so websetdefaultlangcfg function.	2021-02-08	7.2	CVE-2021-25172 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetservicecfg function.	2021-02-08	7.2	CVE-2021-25169 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webifc_setadconfig function.	2021-02-08	7.2	CVE-2021-26570 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg function.	2021-02-08	7.2	CVE-2021-26571 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg function.	2021-02-08	7.2	CVE-2021-26572 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgeneratesslcfg function.	2021-02-08	7.2	CVE-2021-26573 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletevideofile function.	2021-02-08	7.2	CVE-2021-26574 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletesolvideofile function.	2021-02-08	7.2	CVE-2021-26575 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so uploadsshkey function.	2021-02-08	7.2	CVE-2021-26576 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetremoteimageinfo function.	2021-02-08	7.2	CVE-2021-25170 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webupdatecomponent function.	2021-02-08	7.2	CVE-2021-25168 MISC
hpe -- baseboard_management_controller	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so uploadsshkey function.	2021-02-08	7.2	CVE-2021-26577 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
huawei -- ecns280_firmware	There is a denial of service (DoS) vulnerability in eCNS280 versions V100R005C00, V100R005C10. Due to a design defect, remote unauthorized attackers send a large number of specific messages to affected devices, causing system resource exhaustion and web application DoS.	2021-02-06	7.8	CVE-2021-22292 CONFIRM
logitec -- lan-w300n\/pgrb_firmware	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.	2021-02-12	7.7	CVE-2021-20638 MISC MISC
logitec -- lan-w300n\/pgrb_firmware	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.	2021-02-12	7.7	CVE-2021-20639 MISC MISC
logitec -- lan-w300n\/pgrb_firmware	Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute an arbitrary OS command via unspecified vectors.	2021-02-12	7.7	CVE-2021-20640 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
macfromip_project -- macfromip	This affects all versions of package macfromip. The injection point is located in line 66 in macfromip.js.	2021-02-08	7.5	CVE-2020-7786 MISC MISC
microfocus -- operation_bridge_reporter	Remote Code execution vulnerability in Micro Focus Operation Bridge Reporter (OBR) product, affecting version 10.40. The vulnerability could be exploited to allow Remote Code Execution on the OBR server.	2021-02-08	10	CVE-2021-22502 MISC MISC MISC
ncr -- command_center_agent	CMCAgent in NCR Command Center Agent 16.3 on Aloha POS/BOH servers permits the submission of a runCommand parameter (within an XML document sent to port 8089) that enables the remote, unauthenticated execution of an arbitrary command as SYSTEM, as exploited in the wild in 2020 and/or 2021. NOTE: the vendor's position is that exploitation occurs only on devices with a certain "misconfiguration."	2021-02-07	10	CVE-2021-3122 MISC MISC MISC
netmotionsoftware -- netmotion_mobility	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated	2021-02-08	10	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in MvcUtil valueStringToObject.			26914 MISC MISC MISC
netmotionsoftware -- netmotion_mobility	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in RpcServlet.	2021-02-08	10	CVE-2021-26913 MISC MISC MISC
netmotionsoftware -- netmotion_mobility	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in webrepdb StatusServlet.	2021-02-08	10	CVE-2021-26915 MISC MISC MISC
netmotionsoftware -- netmotion_mobility	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in SupportRpcServlet.	2021-02-08	10	CVE-2021-26912 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
node-ps_project -- node-ps	This affects all versions of package node-ps. The injection point is located in line 72 in lib/index.js.	2021-02-08	7.5	CVE-2020-7785 MISC MISC MISC
open-emr -- openemr	The Patient Portal of OpenEMR 5.0.2.1 is affected by a Command Injection vulnerability in /interface/main/backup.php. To exploit the vulnerability, an authenticated attacker can send a POST request that executes arbitrary OS commands via shell metacharacters.	2021-02-07	9	CVE-2020-36243 MISC MISC
panasonic -- video_insight_vms	Video Insight VMS versions prior to 7.8 allows a remote attacker to execute arbitrary code with the system user privilege by sending a specially crafted request.	2021-02-05	10	CVE-2021-20623 MISC MISC
phpok -- phpok	PhpOK 5.4.137 contains a SQL injection vulnerability that can inject an attachment data through SQL, and then call the attachment replacement function through	2021-02-08	7.5	CVE-2020-16629 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	api.php to write a PHP file to the target path.			
set-or-get_project -- set-or-get	Prototype pollution vulnerability in ‘set-or-get’ version 1.0.0 through 1.2.10 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-02-08	7.5	CVE-2021-25913 MISC MISC
siemens -- digsi_4	A vulnerability has been identified in DIGSI 4 (All versions < V4.94 SP1 HF 1). Several folders in the %PATH% are writeable by normal users. As these folders are included in the search for dlls, an attacker could place dlls there with code executed by SYSTEM.	2021-02-09	7.2	CVE-2020-25245 MISC MISC
siemens -- simatic_hmi_comfort_panels_firmware	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V16 Update 3a), SIMATIC HMI KTP Mobile Panels (All versions < V16 Update 3a). Affected devices with enabled telnet service do not require authentication for this service. This could allow a remote	2021-02-09	9.3	CVE-2020-15798 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to gain full access to the device. (ZDI-CAN-12046)			
siemens -- simatic_process_control_system_neo	A vulnerability has been identified in PCS neo (Administration Console) (V3.0), TIA Portal (V15, V15.1 and V16). Manipulating certain files in specific folders could allow a local attacker to execute code with SYSTEM privileges. The security vulnerability could be exploited by an attacker with a valid account and limited access rights on the system.	2021-02-09	7.2	CVE-2020-25238 MISC MISC CERT-VN
spritesheet-js_project -- spritesheet-js	This affects all versions of package spritesheet-js. It depends on a vulnerable package platform-command. The injection point is located in line 32 in lib/generator.js, which is triggered by main entry of the package.	2021-02-08	7.5	CVE-2020-7782 MISC MISC MISC
svakom -- siime_eye_firmware	An issue was discovered in Svakom Siime Eye 14.1.00000001.3.330.0.0.3.14. A command injection vulnerability resides in the HOST/IP section of the NFS settings menu in the webserver running on the	2021-02-08	10	CVE-2020-11920 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. By injecting Bash commands via shell metacharacters here, the device executes arbitrary code with root privileges (all of the device's services are running as root).			
wavlink -- wn575a4_firmware	Wavlink WN575A4 and WN579X3 devices through 2020-05-15 allow unauthenticated remote users to inject commands via the key parameter in a login request.	2021-02-09	10	CVE-2020-13117 MISC
wpdatatables -- wpdatatables	wpDataTables before 3.4.1 mishandles order direction for server-side tables, aka admin-ajax.php?action=get_wdtable order[0][dir] SQL injection.	2021-02-08	10	CVE-2021-26754 MISC MISC MISC
zulip -- zulip_desktop	Zulip Desktop before 5.0.0 improperly uses shell.openExternal and shell.openItem with untrusted content, leading to remote code execution.	2021-02-05	7.5	CVE-2020-10857 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zzzcms -- zzzphp	SQL Injection in ZZZCMS zzzphp 1.7.1 allows remote attackers to execute arbitrary code due to a lack of parameter filtering in inc/zzz_template.php.	2021-02-05	7.5	CVE-2020-18717 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1password -- scim_bridge	1Password SCIM Bridge before 1.6.2 mishandles validation of authenticated requests for log files, leading to disclosure of a TLS private key.	2021-02-08	4	CVE-2021-26905 MISC CONFIRM
adminer -- adminer	Adminer through 4.7.8 allows XSS via the history parameter to the default URI.	2021-02-09	4.3	CVE-2020-35572

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21017 MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21028 MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21033 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21035 MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21036 MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21037 MISC
adobe -- acrobat	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	2021-02-11	6.8	CVE-2021-21038 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21039 MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21040 MISC
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21041 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	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.	2021-02-11	6.8	CVE-2021-21021 MISC
adobe -- acrobat	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.	2021-02-11	4.3	CVE-2021-21034 MISC
adobe -- acrobat	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.	2021-02-11	4.3	CVE-2021-21061 MISC
adobe -- acrobat	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	2021-02-11	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			21060 MISC
adobe -- acrobat	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.	2021-02-11	4.3	CVE-2021-21057 MISC
adobe -- acrobat	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.	2021-02-11	4.3	CVE-2021-21046 MISC
adobe -- acrobat	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 escalate privileges	2021-02-11	4.3	CVE-2021-21042 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
advantech -- iview	Advantech iView versions prior to v5.7.03.6112 are vulnerable to directory traversal, which may allow an attacker to read sensitive files.	2021-02-11	5	CVE-2021-22656 MISC MISC
advantech -- iview	Advantech iView versions prior to v5.7.03.6112 are vulnerable to a SQL injection, which may allow an unauthorized attacker to disclose information.	2021-02-11	5	CVE-2021-22654 MISC MISC MISC
apache -- activemq	An instance of a cross-site scripting vulnerability was identified to be present in the web based administration console on the message.jsp page of Apache ActiveMQ versions 5.15.12 through 5.16.0.	2021-02-08	4.3	CVE-2020-13947 MISC MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apostrophecms -- sanitize-html	Apostrophe Technologies sanitize-html before 2.3.1 does not properly handle internationalized domain name (IDN) which could allow an attacker to bypass hostname whitelist validation set by the "allowedIframeHostnames" option.	2021-02-08	5	CVE-2021-26539 MISC MISC
apostrophecms -- sanitize-html	Apostrophe Technologies sanitize-html before 2.3.2 does not properly validate the hostnames set by the "allowedIframeHostnames" option when the "allowIframeRelativeUrls" is set to true, which allows attackers to bypass hostname whitelist for iframe element, related using an src value that starts with "/\\example.com".	2021-02-08	5	CVE-2021-26540 MISC MISC
b2evolution -- b2evolution	Open redirect vulnerability in b2evolution CMS version prior to 6.11.6 allows an attacker to perform malicious open redirects to an attacker controlled resource via redirect_to parameter in email_passthrough.php.	2021-02-09	5.8	CVE-2020-22840 MISC MISC MISC
b2evolution -- b2evolution_cms	Reflected cross-site scripting vulnerability (XSS) in the evoadm.php file in b2evolution cms version 6.11.6-stable allows remote attackers to inject arbitrary webscript or HTML code via the tab3 parameter.	2021-02-09	4.3	CVE-2020-22839 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
carrierwave_project -- carrierwave	CarrierWave is an open-source RubyGem which provides a simple and flexible way to upload files from Ruby applications. In CarrierWave before versions 1.3.2 and 2.1.1 the download feature has an SSRF vulnerability, allowing attacks to provide DNS entries or IP addresses that are intended for internal use and gather information about the Intranet infrastructure of the platform. This is fixed in versions 1.3.2 and 2.1.1.	2021-02-08	4	CVE-2021-21288 MISC MISC MISC CONFIRM MISC
cesanta -- mongoose	The mg_http_serve_file function in Cesanta Mongoose HTTP server 7.0 is vulnerable to remote OOB write attack via connection request after exhausting memory pool.	2021-02-08	6.4	CVE-2021-26528 MISC
cesanta -- mongoose	The mg_tls_init function in Cesanta Mongoose HTTPS server 7.0 and 6.7-6.18 (compiled with mbedTLS support) is vulnerable to remote OOB write attack via connection request after exhausting memory pool.	2021-02-08	6.4	CVE-2021-26529 MISC
cesanta -- mongoose	The mg_tls_init function in Cesanta Mongoose HTTPS server 7.0 (compiled with OpenSSL support) is vulnerable to remote OOB write attack via connection request after exhausting memory pool.	2021-02-08	6.4	CVE-2021-26530 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chainsafe -- ethermint	Cosmos Network Ethermint <= v0.4.0 is affected by cache lifecycle inconsistency in the EVM module. Due to the inconsistency between the Storage caching cycle and the Tx processing cycle, Storage changes caused by a failed transaction are improperly reserved in memory. Although the bad storage cache data will be discarded at EndBlock, it is still valid in the current block, which enables many possible attacks such as an "arbitrary mint token".	2021-02-08	5	CVE-2021-25837 MISC
chainsafe -- ethermint	Cosmos Network Ethermint <= v0.4.0 is affected by a cross-chain transaction replay vulnerability in the EVM module. Since ethermint uses the same chainIDEpoch and signature schemes with ethereum for compatibility, a verified signature in ethereum is still valid in ethermint with the same msg content and chainIDEpoch, which enables "cross-chain transaction replay" attack.	2021-02-08	5	CVE-2021-25835 MISC MISC
chainsafe -- ethermint	Cosmos Network Ethermint <= v0.4.0 is affected by a transaction replay vulnerability in the EVM module. If the victim sends a very large nonce transaction, the attacker can replay the transaction through the application.	2021-02-08	5	CVE-2021-25834 MISC
chainsafe -- ethermint	Cosmos Network Ethermint <= v0.4.0 is affected by cache lifecycle inconsistency in the EVM module. The bytecode set in a FAILED transaction wrongfully remains in memory(stateObject.code) and is further written to persistent store at the Endblock stage, which may be utilized to build honeypot contracts.	2021-02-08	5	CVE-2021-25836 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cryptography_project -- cryptography	In the cryptography package before 3.3.2 for Python, certain sequences of update calls to symmetrically encrypt multi-GB values could result in an integer overflow and buffer overflow, as demonstrated by the Fernet class.	2021-02-07	6.4	CVE-2020-36242 CONFIRM CONFIRM MISC FEDORA
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.2.0 - 9.1.0 contain a privilege escalation vulnerability. A non-admin user with either ISI_PRIV_LOGIN_CONSOLE or ISI_PRIV_LOGIN_SSH may potentially exploit this vulnerability to read arbitrary data, tamper with system software or deny service to users. Note: no non-admin users or roles have these privileges by default.	2021-02-09	4.6	CVE-2020-26192 MISC
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.1.2 – 9.1.0 contain an issue where the OneFS SMB directory auto-create may erroneously create a directory for a user. A remote unauthenticated attacker may take advantage of this issue to slow down the system.	2021-02-09	5	CVE-2020-26195 MISC
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.1.2 and 8.2.2 contain an Incorrect Permission Assignment for a Critical Resource vulnerability. This may allow a non-admin user with either	2021-02-09	4.6	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ISI_PRIV_LOGIN_CONSOLE or ISI_PRIV_LOGIN_SSH privileges to exploit the vulnerability, leading to compromised cryptographic operations. Note: no non-admin users or roles have these privileges by default.			26194 MISC
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.1.0 - 9.1.0 contain a privilege escalation vulnerability. A user with ISI_PRIV_JOB_ENGINE may use the PermissionRepair job to grant themselves the highest level of RBAC privileges thus being able to read arbitrary data, tamper with system software or deny service to users.	2021-02-09	4.6	CVE-2020-26191 MISC
elecom -- wrc-300febk-a_firmware	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.	2021-02-12	4.3	CVE-2021-20646 MISC MISC
elecom -- wrc-300febk-a_firmware	Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject arbitrary script via unspecified vectors.	2021-02-12	4.3	CVE-2021-20645 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elecom -- wrc-300febk-s_firmware	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.	2021-02-12	4.3	CVE-2021-20647 MISC MISC
elecom -- wrc-300febk-s_firmware	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.	2021-02-12	5.8	CVE-2021-20649 MISC MISC
electriccoin -- zcashd	In Electric Coin Company Zcashd before 2.1.1-1, the time offset between messages could be leveraged to obtain sensitive information about the relationship between a suspected victim's address and an IP address, aka a timing side channel.	2021-02-05	5	CVE-2020-8807 MISC
electriccoin -- zcashd	Electric Coin Company Zcashd before 2.1.1-1 allows attackers to trigger consensus failure and double spending. A valid chain could be incorrectly rejected because timestamp requirements on block headers were not properly enforced.	2021-02-05	5	CVE-2020-8806 MISC
emlog -- emlog	emlog v5.3.1 has full path disclosure vulnerability in t/index.php, which allows an attacker to see the path to the webroot/file.	2021-02-08	5	CVE-2021-3293

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
epikur -- epikur	An issue was discovered in Epikur before 20.1.1. A Glassfish 4.1 server with a default configuration is running on TCP port 4848. No password is required to access it with the administrator account.	2021-02-05	4.6	CVE-2020-10537 MISC
ezxml_project -- ezxml	The ezxml_toxml function in ezxml 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.	2021-02-08	5.8	CVE-2021-26220 MISC
ezxml_project -- ezxml	The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.	2021-02-08	5.8	CVE-2021-26221 MISC
ezxml_project -- ezxml	The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.	2021-02-08	5.8	CVE-2021-26222 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fedoraproject -- fedora	A flaw was found in the default configuration of dnsmasq, as shipped with Fedora versions prior to 31 and in all versions Red Hat Enterprise Linux, where it listens on any interface and accepts queries from addresses outside of its local subnet. In particular, the option `local-service` is not enabled. Running dnsmasq in this manner may inadvertently make it an open resolver accessible from any address on the internet. This flaw allows an attacker to conduct a Distributed Denial of Service (DDoS) against other systems.	2021-02-06	4.3	CVE-2020-14312 MISC
fiberhome -- an5506-04-fa_firmware	An issue was discovered on FiberHome AN5506-04-FA devices with firmware RP2631. There is a gepon password for the gepon account.	2021-02-10	5	CVE-2021-27169 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27170 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27172 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fiberhome -- hg6245d_firmware	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).	2021-02-10	5	CVE-2021-27173 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27167 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a 6GFJdY4aAuUKJjdtSn7d password for the rdsadmin account.	2021-02-10	5	CVE-2021-27168 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_5g.cfg has cleartext passwords and 0644 permissions.	2021-02-10	5	CVE-2021-27176 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The password for the enable command is gpon.	2021-02-10	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				27166 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27165 MISC
fiberhome -- hg6245d_firmware	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+g|u credentials for an ISP.	2021-02-10	5	CVE-2021-27144 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / user1234 credentials for an ISP.	2021-02-10	5	CVE-2021-27143 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27142 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
fiberhome -- hg6245d_firmware	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.)	2021-02-10	5	CVE-2021-27141 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27140 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27139 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_2g.cfg has cleartext passwords and 0644 permissions.	2021-02-10	5	CVE-2021-27175 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. wifi_custom.cfg has cleartext passwords and 0644 permissions.	2021-02-10	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				27174 MISC
fiberhome -- hg6245d_firmware	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.	2021-02-10	5	CVE-2021-27179 MISC
fiberhome -- hg6245d_firmware	An issue was discovered on FiberHome HG6245D devices through RP2613. Some passwords are stored in cleartext in nvram.	2021-02-10	5	CVE-2021-27178 MISC
flowpaper -- pdf2json	Buffer overflow in pdf2json 0.69 allows local users to execute arbitrary code by converting a crafted PDF file.	2021-02-05	4.6	CVE-2020-18750 CONFIRM MISC
fortinet -- fortiweb	An improper neutralization of input during web page generation in FortiWeb GUI interface 6.3.0 through 6.3.7 and version before 6.2.4 may allow an unauthenticated, remote attacker to perform a reflected	2021-02-08	4.3	CVE-2021-22122

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cross site scripting attack (XSS) by injecting malicious payload in different vulnerable API end-points.			CONFIRM
foxitsoftware -- foxit_reader	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.	2021-02-10	6.8	CVE-2020-13548 MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of NEF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11192.	2021-02-09	6.8	CVE-2020-17419 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. 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 NEF files. The issue results from the	2021-02-09	6.8	CVE-2020-17427 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11334.			
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of CR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11230.	2021-02-09	6.8	CVE-2020-17426 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11259.	2021-02-09	6.8	CVE-2020-17425 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11247.	2021-02-09	6.8	CVE-2020-17424 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of ARW files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11196.	2021-02-09	6.8	CVE-2020-17423 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of NEF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write	2021-02-09	6.8	CVE-2020-27857 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11488.			
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11434.	2021-02-09	6.8	CVE-2020-27856 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11433.	2021-02-09	6.8	CVE-2020-27855 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11432.	2021-02-09	6.8	CVE-2020-17436 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZIX files. A crafted id in a channel element can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11197.	2021-02-09	6.8	CVE-2020-17418 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this	2021-02-09	6.8	CVE-2020-17430 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to execute code in the context of the current process. Was ZDI-CAN-11332.			
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of CMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11337.	2021-02-09	4.3	CVE-2020-17429 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of NEF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11194.	2021-02-09	6.8	CVE-2020-17421 MISC MISC
foxitsoftware --	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User	2021-02-09	6.8	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxit_studio_photo	interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11333.			17431 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11358.	2021-02-09	6.8	CVE-2020-17435 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of CMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker	2021-02-09	4.3	CVE-2020-17428 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11336.			
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11356.	2021-02-09	6.8	CVE-2020-17433 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CR2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11335.	2021-02-09	6.8	CVE-2020-17432 MISC MISC
foxitsoftware --	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922.	2021-02-09	6.8	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxit_studio_photo	User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ARW files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11357.			17434 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11195.	2021-02-09	4.3	CVE-2020-17422 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of NEF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can	2021-02-09	4.3	CVE-2020-17420 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11193.			
fusioncharts -- apexcharts	The package apexcharts before 3.24.0 are vulnerable to Cross-site Scripting (XSS) via lack of sanitization of graph legend fields.	2021-02-09	4.3	CVE-2021-23327 CONFIRM CONFIRM CONFIRM CONFIRM
genivia -- gsoap	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.	2021-02-10	5	CVE-2020-13578 MISC
genivia -- gsoap	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.	2021-02-10	5	CVE-2020-13577 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
genivia -- gsoap	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.	2021-02-10	5	CVE-2020-13575 MISC
genivia -- gsoap	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.	2021-02-10	5	CVE-2020-13574 MISC
gitea -- gitea	Stack buffer overflow vulnerability in gitea 1.9.0 through 1.13.1 allows remote attackers to cause a denial of service (crash) via vectors related to a file path.	2021-02-05	5	CVE-2021-3382 MISC
godotengine -- godot_engine	An integer overflow issue exists in Godot Engine up to v3.2 that can be triggered when loading specially crafted.TGA image files. The vulnerability exists in ImageLoaderTGA::load_image() function at line: const size_t buffer_size = (tga_header.image_width * tga_header.image_height) * pixel_size; The bug leads to Dynamic stack buffer overflow. Depending on the context of the application, attack vector can be local or remote, and can lead to code execution and/or system crash.	2021-02-08	6.8	CVE-2021-26825 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
godotengine -- godot_engine	A stack overflow issue exists in Godot Engine up to v3.2 and is caused by improper boundary checks when loading .TGA image files. Depending on the context of the application, attack vector can be local or remote, and can lead to code execution and/or system crash.	2021-02-08	6.8	CVE-2021-26826 MISC MISC
google -- android	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	2021-02-10	6.9	CVE-2021-0333 MISC
google -- android	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	2021-02-10	4.9	CVE-2021-0338 MISC
google -- android	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	2021-02-10	6.9	CVE-2021-0331 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-170731783			
google -- android	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	2021-02-10	4.3	CVE-2021-0335 MISC
google -- android	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	2021-02-10	6.9	CVE-2021-0314 MISC
google -- android	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	2021-02-10	5	CVE-2021-0341 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21128 MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass content security policy via a crafted Chrome Extension.	2021-02-09	6.8	CVE-2021-21127 MISC MISC
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21118 MISC MISC
google -- chrome	Use after free in Media in Google Chrome prior to 88.0.4324.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21119 MISC MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
google -- chrome	Use after free in WebSQL in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21120 MISC MISC
google -- chrome	Use after free in Omnibox in Google Chrome on Linux prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21121 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21122 MISC MISC
google -- chrome	Potential user after free in Speech Recognizer in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21124 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.	2021-02-09	6.8	CVE-2021-21132 MISC MISC
google -- chrome	Use after free in WebRTC in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.	2021-02-09	6.8	CVE-2020-16044 MISC MISC
google -- chrome	Use after free in DevTools in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform a sandbox escape via a crafted file.	2021-02-09	6.8	CVE-2021-21138 MISC MISC
google -- chrome	Uninitialized use in USB in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform out of bounds memory access via via a USB device.	2021-02-09	4.6	CVE-2021-21140 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21148 MISC MISC FEDORA
google -- chrome	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21142 MISC MISC FEDORA
google -- chrome	Heap buffer overflow in Extensions in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	2021-02-09	6.8	CVE-2021-21143 MISC MISC FEDORA
google -- chrome	Use after free in Navigation in Google Chrome prior to 88.0.4324.146 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21146 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC FEDORA
google -- chrome	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	2021-02-09	5.8	CVE-2021-21125 MISC MISC
google -- chrome	Heap buffer overflow in Tab Groups in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	2021-02-09	6.8	CVE-2021-21144 MISC MISC FEDORA
google -- chrome	Use after free in Fonts in Google Chrome prior to 88.0.4324.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-09	6.8	CVE-2021-21145 MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in Cryptohome in Google Chrome prior to 88.0.4324.96 allowed a local attacker to perform OS-level privilege escalation via a crafted file.	2021-02-09	6.9	CVE-2021-21117 MISC MISC
google -- chrome	Inappropriate implementation in Skia in Google Chrome prior to 88.0.4324.146 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21147 MISC MISC FEDORA
google -- chrome	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass file extension policy via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21141 MISC MISC
google -- chrome	Inappropriate implementation in iframe sandbox in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21139 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21137 MISC MISC
google -- chrome	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21136 MISC MISC
google -- chrome	Inappropriate implementation in Performance API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21135 MISC MISC
google -- chrome	Incorrect security UI in Page Info in Google Chrome on iOS prior to 88.0.4324.96 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21134 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in Downloads in Google Chrome prior to 88.0.4324.96 allowed an attacker who convinced a user to download files to bypass navigation restrictions via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21133 MISC MISC
google -- chrome	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21131 MISC MISC
google -- chrome	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21130 MISC MISC
google -- chrome	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21129 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension.	2021-02-09	4.3	CVE-2021-21126 MISC MISC
google -- chrome	Insufficient data validation in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	2021-02-09	4.3	CVE-2021-21123 MISC MISC
gradle -- enterprise_test_distribution_agent	A directory traversal issue was discovered in Gradle gradle-enterprise-test-distribution-agent before 1.3.2, test-distribution-gradle-plugin before 1.3.2, and gradle-enterprise-maven-extension before 1.8.2. A malicious actor (with certain credentials) can perform a registration step such that crafted TAR archives lead to extraction of files into arbitrary filesystem locations.	2021-02-09	5.5	CVE-2021-26719 MISC
helm -- helm	Helm is open-source software which is essentially "The Kubernetes Package Manager". Helm is a tool for managing Charts. Charts are packages of pre-configured Kubernetes resources. In Helm from version 3.0 and before version 3.5.2, there a few cases where data loaded from potentially untrusted sources was not properly sanitized. When a SemVer in the `version` field of a chart is invalid, in some	2021-02-05	4	CVE-2021-21303 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cases Helm allows the string to be used "as is" without sanitizing. Helm fails to properly sanitized some fields present on Helm repository `index.yaml` files. Helm does not properly sanitized some fields in the `plugin.yaml` file for plugins In some cases, Helm does not properly sanitize the fields in the `Chart.yaml` file. By exploiting these attack vectors, core maintainers were able to send deceptive information to a terminal screen running the `helm` command, as well as obscure or alter information on the screen. In some cases, we could send codes that terminals used to execute higher-order logic, like clearing a terminal screen. Further, during evaluation, the Helm maintainers discovered a few other fields that were not properly sanitized when read out of repository index files. This fix remedies all such cases, and once again enforces SemVer2 policies on version fields. All users of the Helm 3 should upgrade to the fixed version 3.5.2 or later. Those who use Helm as a library should verify that they either sanitize this data on their own, or use the proper Helm API calls to sanitize the data.			CONFIRM
httplib2_project -- httplib2	httplib2 is a comprehensive HTTP client library for Python. In httplib2 before version 0.19.0, a malicious server which responds with long series of "\xa0" characters in the "www-authenticate" header may cause Denial of Service (CPU burn while parsing header) of the httplib2 client accessing said server. This is fixed in version 0.19.0 which contains a new implementation of auth headers parsing using the pyparsing library.	2021-02-08	5	CVE-2021-21240 MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- ais-bw80h-00_firmware	There is an insufficient integrity check vulnerability in Huawei Sound X Product. The system does not check certain software package's integrity sufficiently. Successful exploit could allow an attacker to load a crafted software package to the device. Affected product versions include:AIS-BW80H-00 versions 9.0.3.1(H100SP13C00),9.0.3.1(H100SP18C00),9.0.3.1(H100SP3C00),9.0.3.1(H100SP9C00),9.0.3.2(H100SP1C00),9.0.3.2(H100SP2C00),9.0.3.2(H100SP5C00),9.0.3.2(H100SP8C00),9.0.3.3(H100SP1C00).	2021-02-06	4.6	CVE-2020-9118 CONFIRM
huawei -- campusinsight	Some Huawei products have an inconsistent interpretation of HTTP requests vulnerability. Attackers can exploit this vulnerability to cause information leak. Affected product versions include: CampusInsight versions V100R019C10; ManageOne versions 6.5.1.1, 6.5.1.SPC100, 6.5.1.SPC200, 6.5.1RC1, 6.5.1RC2, 8.0.RC2. Affected product versions include: Taurus-AL00A versions 10.0.0.1(C00E1R1P1).	2021-02-06	5	CVE-2021-22293 CONFIRM
huawei -- imaster_mae-m	There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. Affected product versions include: ManageOne versions 6.5.0,6.5.0.SPC100.B210,6.5.1.1.B010,6.5.1.1.B020,6.5.1.1.B030,6.5.1.1.B040,6.5.1.SPC100.B050,6.5.1.SPC101.B010,6.5.1.SPC101.B040,6.5.1.SPC200,6.5.1.SPC200.B010,6.5.1.SPC200.B030,6.5.1.SPC200.B040,6.5.1.SPC200.B050,6.5.1.SPC200.B060,6.5.1.SPC200.B070,	2021-02-06	4.6	CVE-2021-22299 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	6.5.1RC1.B060,6.5.1RC2.B020,6.5.1RC2.B030,6.5.1RC2.B040,6.5.1RC2.B050,6.5.1RC2.B060,6.5.1RC2.B070,6.5.1RC2.B080,6.5.1RC2.B090,6.5.RC2.B050,8.0.0,8.0.0-LCND81,8.0.0.SPC100,8.0.1,8.0.RC2,8.0.RC3,8.0.RC3.B041,8.0.RC3.SPC100; NFV_FusionSphere versions 6.5.1.SPC23,8.0.0.SPC12; SMC2.0 versions V600R019C00,V600R019C10; iMaster MAE-M versions MAE-TOOL(FusionSphereBasicTemplate_Euler_X86)V100R020C10SPC220.			
huawei -- manageone	There is a logic vulnerability in Huawei Gauss100 OLTP Product. An attacker with certain permissions could perform specific SQL statement to exploit this vulnerability. Due to insufficient security design, successful exploit can cause service abnormal. Affected product versions include: ManageOne versions 6.5.1.1.B020, 6.5.1.1.B030, 6.5.1.1.B040, 6.5.1.SPC100.B050, 6.5.1.SPC101.B010, 6.5.1.SPC101.B040, 6.5.1.SPC200, 6.5.1.SPC200.B010, 6.5.1.SPC200.B030, 6.5.1.SPC200.B040, 6.5.1.SPC200.B050, 6.5.1.SPC200.B060, 6.5.1.SPC200.B070, 6.5.1RC1.B070, 6.5.1RC1.B080, 6.5.1RC2.B040, 6.5.1RC2.B050, 6.5.1RC2.B060, 6.5.1RC2.B070, 6.5.1RC2.B080, 6.5.1RC2.B090.	2021-02-06	4	CVE-2021-22298 CONFIRM
huawei -- manageone	There has a CSV injection vulnerability in ManageOne 8.0.1. An attacker with common privilege may exploit this vulnerability through some operations to inject the CSV files. Due to insufficient	2021-02-06	4	CVE-2020-9205 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	input validation of some parameters, the attacker can exploit this vulnerability to inject CSV files to the target device.			
huawei -- mate_30_firmware	Mate 30 10.0.0.203(C00E201R7P2) have a buffer overflow vulnerability. After obtaining the root permission, an attacker can exploit the vulnerability to cause buffer overflow.	2021-02-06	4.6	CVE-2021-22301 CONFIRM
huawei -- taurus-al00a_firmware	There is a pointer double free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). There is a lack of muti-thread protection when a function is called. Attackers can exploit this vulnerability by performing malicious operation to cause pointer double free. This may lead to module crash, compromising normal service.	2021-02-06	4.3	CVE-2021-22303 CONFIRM
ibm -- cloud_pak_for_automation	IBM Cloud Pak for Automation 20.0.3, 20.0.2-IF002 - Business Automation Application Designer Component stores potentially sensitive information in log files that could be obtained by an unauthorized user. IBM X-Force ID: 194966.	2021-02-08	4	CVE-2021-20359 XF CONFIRM
ibm -- cloud_pak_f	IBM Cloud Pak for Automation 20.0.3, 20.0.2-IF002 stores potentially sensitive information in clear text in API connection log	2021-02-08	4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
or_automation	files. This information could be obtained by a user with permissions to read log files. IBM X-Force ID: 194965.			20358 XF CONFIRM
ibm -- security_identity_governance_and_intelligence	IBM Security Identity Governance and Intelligence 5.2.6 could disclose sensitive information to an unauthorized user using a specially crafted HTTP request. IBM X-Force ID: 189446.	2021-02-09	6.4	CVE-2020-4795 XF CONFIRM
ibm -- security_identity_governance_and_intelligence	IBM Security Identity Governance and Intelligence 5.2.6 does not invalidate session after logout which could allow a user to obtain sensitive information from another users' session. IBM X-Force ID: 192912.	2021-02-09	5	CVE-2020-4995 XF CONFIRM
ibm -- security_verify_information_queue	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.	2021-02-11	5	CVE-2021-20404 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_information_queue	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.	2021-02-11	5	CVE-2021-20405 XF CONFIRM
ibm -- security_verify_information_queue	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: 198185.	2021-02-12	5	CVE-2021-20407 XF CONFIRM
ibm -- security_verify_information_queue	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: 198188.	2021-02-12	5	CVE-2021-20409 XF CONFIRM
ibm -- security_verify_information_queue	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.	2021-02-11	6.8	CVE-2021-20403 XF

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
				CONFIRM
ibm -- security_verify_information_queue	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: 198184.	2021-02-12	4	CVE-2021-20406 XF CONFIRM
ibm -- security_verify_information_queue	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.	2021-02-11	4	CVE-2021-20402 XF CONFIRM
ibm -- security_verify_information_queue	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.	2021-02-12	5	CVE-2021-20412 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_information_queue	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.	2021-02-12	4.8	CVE-2021-20411 XF CONFIRM
ibm -- spectrum_protect_plus	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.	2021-02-10	5	CVE-2020-5023 XF CONFIRM
ibm -- websphere_application_server	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.	2021-02-10	6.4	CVE-2021-20353 XF CONFIRM MISC
imagely -- nextgen_gallery	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload. (It is possible to bypass CSRF protection by simply not including a nonce parameter.)	2021-02-09	4.3	CVE-2020-35943 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
imagely -- nextgen_gallery	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload and Local File Inclusion via settings modification, leading to Remote Code Execution and XSS. (It is possible to bypass CSRF protection by simply not including a nonce parameter.)	2021-02-09	6.8	CVE-2020-35942 MISC
imagemagick -- imagemagick	A flaw was found in ImageMagick in MagickCore/gem.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.10-56.	2021-02-06	6.8	CVE-2021-20176 MISC
iobit -- advanced_systemcare	The AscRegistryFilter.sys kernel driver in IObit Advanced SystemCare 13.2 allows an unprivileged user to send an IOCTL to the device driver. If the user provides a NULL entry for the dwIoControlCode parameter, a kernel panic (aka BSOD) follows. The IOCTL codes can be found in the dispatch function: 0x8001E000, 0x8001E004, 0x8001E008, 0x8001E00C, 0x8001E010, 0x8001E014, 0x8001E020, 0x8001E024, 0x8001E040, 0x8001E044, and 0x8001E048. \DosDevices\AscRegistryFilter and \Device\AscRegistryFilter are affected.	2021-02-05	6.8	CVE-2020-10234 MISC MISC MISC
jenzabar -- jenzabar	Jenzabar 9.2.x through 9.2.2 allows /ics?tool=search&query= XSS.	2021-02-06	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				26723 MISC MISC MISC
librenms -- librenms	A second-order SQL injection issue in Widgets/TopDevicesController.php (aka the Top Devices dashboard widget) of LibreNMS before 21.1.0 allows remote authenticated attackers to execute arbitrary SQL commands via the sort_order parameter against the /ajax/form/widget-settings endpoint.	2021-02-08	6.5	CVE-2020-35700 MISC MISC CONFIRM CONFIRM MISC
linkedin -- oncall	LinkedIn Oncall through 1.4.0 allows reflected XSS via /query because of mishandling of the "No results found for" message in the search bar.	2021-02-05	4.3	CVE-2021-26722 MISC
linux -- linux_kernel	A local privilege escalation was discovered in the Linux kernel before 5.10.13. Multiple race conditions in the AF_VSOCK implementation are caused by wrong locking in net/vmw_vsock/af_vsock.c. The race	2021-02-05	6.9	CVE-2021-26708 MLIST

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	conditions were implicitly introduced in the commits that added VSOCK multi-transport support.			MISC MISC MISC
marked_project -- marked	Marked is an open-source markdown parser and compiler (npm package "marked"). In marked from version 1.1.1 and before version 2.0.0, there is a Regular expression Denial of Service vulnerability. This vulnerability can affect anyone who runs user generated code through marked. This vulnerability is fixed in version 2.0.0.	2021-02-08	5	CVE-2021-21306 MISC MISC MISC CONFIRM MISC
maxpcsecure -- max_spyware_detector	In Max Secure Max Spyware Detector 1.0.0.044, the driver file (MaxProc64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x2200019. (This also extends to the various other products from Max Secure that include MaxProc64.sys.)	2021-02-05	4.6	CVE-2020-12122 MISC MISC MISC
mcafee -- endpoint_security	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	2021-02-10	4.9	CVE-2021-23883

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system call which is not handled correctly. This varies by machine and had partial protection prior to this update.			CONFIRM
mcafee -- total_protection	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.	2021-02-10	4.6	CVE-2021-23874 CONFIRM
microfocus -- application_performance_management	Cross Site Request Forgery vulnerability in Micro Focus Application Performance Management product, affecting versions 9.40, 9.50 and 9.51. The vulnerability could be exploited by attacker to trick the users into executing actions of the attacker's choosing.	2021-02-06	4.3	CVE-2021-22500 CONFIRM
millewin -- millewin	Millennium Millewin (also known as "Cartella clinica") 13.39.028, 13.39.28.3342, and 13.39.146.1 has insecure folder permissions allowing a malicious user for a local privilege escalation.	2021-02-09	6.5	CVE-2021-3394 MISC MISC
ms3d_project -- ms3d	An issue was discovered in the ms3d crate before 0.1.3 for Rust. It might allow attackers to obtain sensitive information from uninitialized memory locations via IoReader::read.	2021-02-09	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				26952 MISC
name_directory_project -- name_directory	Cross-site request forgery (CSRF) vulnerability in Name Directory 1.17.4 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-02-05	6.8	CVE-2021-20652 MISC MISC
nedi -- nedi	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.	2021-02-12	6.5	CVE-2021-26753 MISC
nedi -- nedi	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.	2021-02-12	4	CVE-2021-26751 MISC
nedi -- nedi	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	2021-02-12	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to obtain access to the operating system where NeDi is installed and to all application data.			26752 MISC
nopcommerce -- nopcommerce	In nopCommerce 4.30, a Reflected XSS issue in the Discount Coupon component allows remote attackers to inject arbitrary web script or HTML through the Filters/CheckDiscountCouponAttribute.cs discountcode parameter.	2021-02-08	4.3	CVE-2021-26916 MISC
octobercms -- october	An issue was discovered in October through build 471. It reactivates an old session ID (which had been invalid after a logout) once a new login occurs. NOTE: this violates the intended Auth/Manager.php authentication behavior but, admittedly, is only relevant if an old session ID is known to an attacker.	2021-02-05	6.8	CVE-2021-3311 CONFIRM MISC
omron -- cx-one	The Omron CX-One Version 4.60 and prior is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.	2021-02-09	6.8	CVE-2020-27261 MISC MISC MISC
omron -- cx-one	The Omron CX-One Version 4.60 and prior may allow an attacker to supply a pointer to arbitrary memory locations, which may allow an attacker to remotely execute arbitrary code.	2021-02-09	6.8	CVE-2020-27259

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
omron -- cx-one	This vulnerability allows local attackers to execute arbitrary code due to the lack of proper validation of user-supplied data, which can result in a type-confusion condition in the Omron CX-One Version 4.60 and prior devices.	2021-02-09	6.8	CVE-2020-27257 MISC MISC
opmantek -- open-audit	Opmantek Open-AudIT 4.0.1 is affected by cross-site scripting (XSS). When outputting SQL statements for debugging, a maliciously crafted query can trigger an XSS attack. This attack only succeeds if the user is already logged in to Open-AudIT before they click the malicious link.	2021-02-05	4.3	CVE-2021-3333 MISC
otrs -- cis_in_customer_frontend	Agents are able to see and link Config Items without permissions, which are defined in General Catalog. This issue affects: OTRS AG OTRSCIsInCustomerFrontend 7.0.x version 7.0.14 and prior versions.	2021-02-08	4	CVE-2021-21436 CONFIRM
otrs -- otrs	Article Bcc fields and agent personal information are shown when customer prints the ticket (PDF) via external interface. This issue	2021-02-08	4.3	CVE-2021-21435

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affects: OTRS AG OTRS 7.0.x version 7.0.23 and prior versions; 8.0.x version 8.0.10 and prior versions.			CONFIRM
otrs -- ticket_forms	When dynamic templates are used (OTRSTicketForms), admin can use OTRS tags which are not masked properly and can reveal sensitive information. This issue affects: OTRS AG OTRSTicketForms 6.0.x version 6.0.40 and prior versions; 7.0.x version 7.0.29 and prior versions; 8.0.x version 8.0.3 and prior versions.	2021-02-08	4	CVE-2020-1779 CONFIRM
phpshe -- phpshe	Multiple SQL Injection vulnerabilities in PHPSHE 1.7 in phpshe/admin.php via the (1) ad_id, (2) menu_id, and (3) cashout_id parameters, which could let a remote malicious user execute arbitrary code.	2021-02-09	6.5	CVE-2020-18215 MISC MISC
privateoctopus -- picoquic	picoquic (before 3rd of July 2020) allows attackers to cause a denial of service (infinite loop) via a crafted QUIC frame, related to the picoquic_decode_frames and picoquic_decode_stream_frame functions and epoch==3.	2021-02-08	5	CVE-2020-24944 MISC
psyprax -- psyprax	An issue was discovered in Psyprax beforee 3.2.2. Passwords used to encrypt the data are stored in the database in an obfuscated format,	2021-02-05	5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	which can be easily reverted. For example, the password AAAAAAAA is stored in the database as MMMMMMMM.			10554 MISC
psyprax -- psyprax	An issue was discovered in Psyprax before 3.2.2. The Firebird database is accessible with the default user sysdba and password masterke after installation. This allows any user to access it and read and modify the contents, including passwords. Local database files can be accessed directly as well.	2021-02-05	5.5	CVE-2020-10552 MISC
redwood -- report2web	A cross-site scripting (XSS) issue in the login panel in Redwood Report2Web 4.3.4.5 and 4.5.3 allows remote attackers to inject JavaScript via the signIn.do urll parameter.	2021-02-05	4.3	CVE-2021-26710 MISC
redwood -- report2web	A frame-injection issue in the online help in Redwood Report2Web 4.3.4.5 allows remote attackers to render an external resource inside a frame via the help/Online_Help/NetHelp/default.htm turl parameter.	2021-02-05	5	CVE-2021-26711 MISC
sdgc -- pnpscada	PNPSCADA 2.200816204020 allows cross-site scripting (XSS), which can execute arbitrary JavaScript in the victim's browser.	2021-02-10	4.3	CVE-2020-24842 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- cscape	Cscape (All versions prior to 9.90 SP3.5) lacks proper validation of user-supplied data when parsing project files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute code in the context of the current process.	2021-02-09	6.8	CVE-2021-22663 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing BMP files. This can result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12018)	2021-02-09	4.6	CVE-2020-27000 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12041)	2021-02-09	4.6	CVE-2020-27001 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing TIFF files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this	2021-02-09	4.6	CVE-2020-27003 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to execute code in the context of the current process. (ZDI-CAN-12158)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of TGA files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12178)	2021-02-09	4.6	CVE-2020-27005 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PCT files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12182)	2021-02-09	4.6	CVE-2020-27006 MISC
siemens -- nucleus_net	A vulnerability has been identified in Nucleus NET (All versions < V5.2), Nucleus ReadyStart for ARM, MIPS, and PPC (All versions < V2012.12). Initial Sequence Numbers (ISNs) for TCP connections are derived from an insufficiently random source. As a result, the ISN of current and future TCP connections could be predictable. An attacker could hijack existing sessions or spoof future ones.	2021-02-09	5	CVE-2020-28388 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- simaris_configuration	A vulnerability has been identified in SIMARIS configuration (All versions). During installation to default target folder, incorrect permissions are configured for the application folder and subfolders which could allow an attacker to gain persistence or potentially escalate privileges should a user with elevated credentials log onto the machine.	2021-02-09	4.6	CVE-2020-28392 MISC
sthttpd_project -- sthttpd	An issue was discovered in sthttpd through 2.27.1. On systems where the strcpy function is implemented with memcpy, the de_dotdot function may cause a Denial-of-Service (daemon crash) due to overlapping memory ranges being passed to memcpy. This can triggered with an HTTP GET request for a crafted filename. NOTE: this is similar to CVE-2017-10671, but occurs in a different part of the de_dotdot function.	2021-02-07	5	CVE-2021-26843 MISC
svakom -- siime_eye_firmware	An issue was discovered in Svakom Siime Eye 14.1.00000001.3.330.0.0.3.14. By sending a set_params.cgi?telnetd=1&save=1&reboot=1 request to the webserver, it is possible to enable the telnet interface on the device. The telnet interface can then be used to obtain access to the device with root privileges via a reecam4debug default password. This default telnet password is the same across all Siime Eye devices. In order for the attack to be exploited, an attacker must be physically close in order to connect to the device's Wi-Fi access point.	2021-02-08	4.6	CVE-2020-11915 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
symonics -- libmysofa	Incorrect handling of input data in verifyAttribute function in the libmysofa library 0.5 - 1.1 will lead to NULL pointer dereference and segmentation fault error in case of restrictive memory protection or near NULL pointer overwrite in case of no memory restrictions (e.g. in embedded environments).	2021-02-08	4.3	CVE-2020-36148 MISC
symonics -- libmysofa	Incorrect handling of input data in changeAttribute function in the libmysofa library 0.5 - 1.1 will lead to NULL pointer dereference and segmentation fault error in case of restrictive memory protection or near NULL pointer overwrite in case of no memory restrictions (e.g. in embedded environments).	2021-02-08	4.3	CVE-2020-36149 MISC
symonics -- libmysofa	Incorrect handling of input data in loudness function in the libmysofa library 0.5 - 1.1 will lead to heap buffer overflow and access to unallocated memory block.	2021-02-08	4.3	CVE-2020-36150 MISC
symonics -- libmysofa	Incorrect handling of input data in mysofa_resampler_reset_mem function in the libmysofa library 0.5 - 1.1 will lead to heap buffer overflow and overwriting large memory block.	2021-02-08	4.3	CVE-2020-36151 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
symonics -- libmysofa	Buffer overflow in readDataVar in hdf/dataobject.c in Symonics libmysofa 0.5 - 1.1 allows attackers to execute arbitrary code via a crafted SOFA.	2021-02-08	6.8	CVE-2020-36152 MISC
tenable -- nessus_amazon_machine_image	Nessus AMI versions 8.12.0 and earlier were found to either not validate, or incorrectly validate, a certificate which could allow an attacker to spoof a trusted entity by using a man-in-the-middle (MITM) attack.	2021-02-06	4.3	CVE-2020-5812 MISC
tipsandtricks-hq -- wp_security_\&_firewall	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.	2021-02-10	4.3	CVE-2020-29171 CONFIRM CONFIRM MISC
tufin -- securetrack	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities were present in Tufin SecureTrack, affecting all versions prior to R20-2 GA.	2021-02-09	6.8	CVE-2020-13460 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tufin -- securetrack	Tufin SecureTrack < R20-2 GA contains reflected + stored XSS (as in, the value is reflected back to the user, but is also stored within the DB and can be later triggered again by the same victim, or also later by different users). Both stored, and reflected payloads are triggerable by admin, so malicious non-authenticated user could get admin level access. Even malicious low-privileged user can inject XSS, which can be executed by admin, potentially elevating privileges and obtaining admin access. (issue 1 of 3)	2021-02-09	4.3	CVE-2020-13407 MISC
tufin -- securetrack	Tufin SecureTrack < R20-2 GA contains reflected + stored XSS (as in, the value is reflected back to the user, but is also stored within the DB and can be later triggered again by the same victim, or also later by different users). Both stored, and reflected payloads are triggerable by admin, so malicious non-authenticated user could get admin level access. Even malicious low-privileged user can inject XSS, which can be executed by admin, potentially elevating privileges and obtaining admin access. (issue 2 of 3)	2021-02-09	4.3	CVE-2020-13408 MISC
tufin -- securetrack	Tufin SecureTrack < R20-2 GA contains reflected + stored XSS (as in, the value is reflected back to the user, but is also stored within the DB and can be later triggered again by the same victim, or also later by different users). Both stored, and reflected payloads are triggerable by admin, so malicious non-authenticated user could get admin level access. Even malicious low-privileged user can inject XSS, which can be executed by admin, potentially elevating privileges and obtaining admin access. (issue 3 of 3)	2021-02-09	4.3	CVE-2020-13409 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tufin -- securetrack	Insecure Direct Object Reference (IDOR) exists in Tufin SecureChange, affecting all versions prior to R20-2 GA. Fixed in version R20-2 GA.	2021-02-09	5	CVE-2020-13462 MISC
typora -- typora	An issue was discovered in Typora 0.9.67. There is an XSS vulnerability that causes Remote Code Execution.	2021-02-05	4.3	CVE-2020-18737 MISC
zohocorp -- manageengine_applications_manager	doFilter in com.adventnet.appmanager.filter.UriCollector in Zoho ManageEngine Applications Manager through 14930 allows an authenticated SQL Injection via the resourceid parameter to showresource.do.	2021-02-05	6.5	CVE-2020-35765 MISC CONFIRM CONFIRM CONFIRM
zulip -- zulip_desktop	Zulip Desktop before 5.0.0 allows attackers to perform recording via the webcam and microphone due to a missing permission request handler.	2021-02-05	5	CVE-2020-10858

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
b2evolution -- b2evolution	Stored XSS in b2evolution CMS version 6.11.6 and prior allows an attacker to perform malicious JavaScript code execution via the plugin name input field in the plugin module.	2021-02-09	3.5	CVE-2020-22841 MISC MISC MISC
casap_automated_enrollment_system_project -- casap_automated_enrollment_system	CASAP Automated Enrollment System 1.0 is affected by cross-site scripting (XSS) in users.php. An attacker can steal a cookie to perform user redirection to a malicious website.	2021-02-09	3.5	CVE-2021-3294 MISC MISC MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.1.0-9.1.0 contain a Backup/Restore Privilege implementation issue. A user with the BackupAdmin role may potentially exploit this vulnerability resulting in the ability to write data outside of the intended file system location.	2021-02-09	2.1	CVE-2020-26196 MISC
epikur -- epikur	An issue was discovered in Epikur before 20.1.1. It stores the secret passwords of the users as MD5 hashes in the database. MD5 can be brute-forced efficiently and should not be used for such purposes. Additionally, since no salt is used, rainbow tables can speed up the attack.	2021-02-05	2.1	CVE-2020-10538 MISC
epson -- iprojection	In Epson iProjection v2.30, the driver file (EMP_NSAU.sys) allows local users to cause a denial of service (BSOD) via crafted input to the virtual audio device driver with IOCTL 0x9C402402, 0x9C402406, or 0x9C40240A.	2021-02-05	2.1	CVE-2020-9014 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	\Device\EMPNSAUIO and \DosDevices\EMPNSAU are similarly affected.			
epson -- iprojection	In Epson iProjection v2.30, the driver file EMP_MPAU.sys allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9C402406 and IOCtl 0x9C40240A. (0x9C402402 has only a NULL pointer dereference.) This affects \Device\EMPMPAUIO and \DosDevices\EMPMPAU.	2021-02-05	2.1	CVE-2020-9453 MISC MISC MISC
gnome -- control_center	A flaw was found in the GNOME Control Center in Red Hat Enterprise Linux 8 versions prior to 8.2, where it improperly uses Red Hat Customer Portal credentials when a user registers a system through the GNOME Settings User Interface. This flaw allows a local attacker to discover the Red Hat Customer Portal	2021-02-08	2.1	CVE-2020-14391 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	password. The highest threat from this vulnerability is to confidentiality.			
gnome -- gnome-autoar	autoar-extractor.c in GNOME gnome-autoar through 0.2.4, as used by GNOME Shell, Nautilus, and other software, allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink to a directory outside of the intended extraction location.	2021-02-05	2.1	CVE-2020-36241 MISC MISC
google -- android	OPPO Android Phone with MTK chipset and Android 8.1/9/10/11 versions have an information leak vulnerability. The “adb shell getprop ro.vendor.aee.enforcing” or “adb shell getprop ro.vendor.aee.enforcing” return no.	2021-02-06	2.1	CVE-2020-11836 MISC
henriquedornas -- henriquedornas	A stored XSS issue exists in henriquedornas 5.2.17 via online live chat.	2021-02-10	3.5	CVE-2021-26938 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- ecns280_td_firmware	There is an information leak vulnerability in eCNS280_TD versions V100R005C00 and V100R005C10. A command does not have timeout exit mechanism. Temporary file contains sensitive information. This allows attackers to obtain information by inter-process access that requires other methods.	2021-02-06	1.9	CVE-2021-22300 CONFIRM
huawei -- mate_30_firmware	There is a buffer overflow vulnerability in Mate 30 10.1.0.126(C00E125R5P3). A module does not verify the some input when dealing with messages. Attackers can exploit this vulnerability by sending malicious input through specific module. This could cause buffer overflow, compromising normal service.	2021-02-06	2.1	CVE-2021-22305 CONFIRM
huawei -- mate_30_firmware	There is an out-of-bound read vulnerability in Mate 30 10.0.0.182(C00E180R6P2). A module does not verify the some input when dealing with messages.	2021-02-06	2.1	CVE-2021-22306 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Attackers can exploit this vulnerability by sending malicious input through specific module. This could cause out-of-bound, compromising normal service.			
huawei -- mate_30_firmware	There is a weak algorithm vulnerability in Mate 3010.0.0.203(C00E201R7P2). The protection is insufficient for the modules that should be protected. Local attackers can exploit this vulnerability to affect the integrity of certain module.	2021-02-06	2.1	CVE-2021-22307 CONFIRM
huawei -- taurus-al00a_firmware	There is a use after free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module may refer to some memory after it has been freed while dealing with some messages. Attackers can exploit this vulnerability by sending specific message to the affected module. This may lead to module crash, compromising normal service.	2021-02-06	2.1	CVE-2021-22304 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- taurus-al00a_firmware	There is an out-of-bound read vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module does not verify the some input. Attackers can exploit this vulnerability by sending malicious input through specific app. This could cause out-of-bound, compromising normal service.	2021-02-06	3.6	CVE-2021-22302 MISC
ibm -- business_automation_workflow	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.	2021-02-11	3.5	CVE-2020-4768 XF CONFIRM
ibm -- powerha	IBM PowerHA 7.2 could allow a local attacker to obtain sensitive information from temporary directories after a discovery failure occurs. IBM X-Force ID: 189969.	2021-02-05	2.1	CVE-2020-4832 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
ibm -- security_identity_governance_and_intelligence	IBM Security Identity Governance and Intelligence 5.2.6 could allow a local user to obtain sensitive information via the capturing of screenshots of authentication credentials. IBM X-Force ID: 192913.	2021-02-09	2.1	CVE-2020-4996 XF CONFIRM
ibm -- security_identity_governance_and_intelligence	IBM Security Identity Governance and Intelligence 5.2.6 could allow an attacker to obtain sensitive information using main in the middle attacks due to improper certificate validation. IBM X-Force ID: 189379.	2021-02-09	1.8	CVE-2020-4791 XF CONFIRM
ibm -- security_identity_governance_and_intelligence	IBM Security Identity Governance and Intelligence 5.2.6 could allow a user to cause a denial of service due to improperly validating a supplied URL, rendering the application unusuable. IBM X-Force ID: 189375.	2021-02-09	3.3	CVE-2020-4790 XF CONFIRM

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
ibm -- security_verify_information_queue	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.	2021-02-12	2.1	CVE-2021-20408 XF CONFIRM
ibm -- security_verify_information_queue	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.	2021-02-12	3.5	CVE-2021-20410 XF CONFIRM
mcafee -- endpoint_security	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.	2021-02-10	3.5	CVE-2021-23881 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mcafee -- endpoint_security	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.	2021-02-10	1.9	CVE-2021-23882 CONFIRM
mcafee -- endpoint_security	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.	2021-02-10	2.1	CVE-2021-23880 CONFIRM
microfocus -- application_performance_management	Persistent Cross-Site scripting vulnerability in Micro Focus Application Performance	2021-02-06	3.5	CVE-2021-22499

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Management product, affecting versions 9.40, 9.50 and 9.51. The vulnerability could allow persistent XSS attack.			CONFIRM
netapp -- clustered_data_ontap	Clustered Data ONTAP versions prior to 9.1P18 and 9.3P12 are susceptible to a vulnerability which could allow an attacker to discover node names via AutoSupport bundles even when the –remove-private-data parameter is set to true.	2021-02-08	2.1	CVE-2020-8590 MISC
netapp -- clustered_data_ontap	Clustered Data ONTAP versions prior to 9.3P20 are susceptible to a vulnerability which could allow an attacker to discover node names via AutoSupport bundles even when the –remove-private-data parameter is set to true.	2021-02-08	2.1	CVE-2020-8578 MISC
netapp -- oncommand_system_manager	OnCommand System Manager 9.x versions prior to 9.3P20 and 9.4 prior to 9.4P3 are susceptible to a vulnerability that could allow HTTP	2021-02-08	2.1	CVE-2020-8587 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	clients to cache sensitive responses making them accessible to an attacker who has access to the system where the client runs.			
newmediacompany -- smarty	An issue was discovered in New Media Smarty before 9.10. Passwords are stored in the database in an obfuscated format that can be easily reversed. The file data.mdb contains these obfuscated passwords in the second column. NOTE: this is unrelated to the popular Smarty template engine product.	2021-02-05	2.1	CVE-2020-10375 MISC MISC
nvidia -- geforce_experience	NVIDIA GeForce Experience, all versions prior to 3.21, contains a vulnerability in GameStream (rxdiag.dll) where an arbitrary file deletion due to improper handling of log files may lead to denial of service.	2021-02-05	3.6	CVE-2021-1072 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
online_marriage_registration_system_project -- online_marriage_registration_system	Online Marriage Registration System 1.0 is affected by stored cross-site scripting (XSS) vulnerabilities in multiple parameters.	2021-02-08	3.5	CVE-2020-26052 MISC
openwrt -- openwrt	In OpenWrt 19.07.x before 19.07.7, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. This affects the netifd and odhcp6c packages.	2021-02-07	3.3	CVE-2021-22161 CONFIRM
otrs -- survey	Survey administrator can craft a survey in such way that malicious code can be executed in the agent interface (i.e. another agent who wants to make changes in the survey). This issue affects: OTRS	2021-02-08	3.5	CVE-2021-21434 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	AG Survey 6.0.x version 6.0.20 and prior versions; 7.0.x version 7.0.19 and prior versions.			
psyprax -- psyprax	An issue was discovered in Psyprax before 3.2.2. The file %PROGRAMDATA%\Psyprax32\PPScreen.ini contains a hash for the lockscreen (aka screensaver) of the application. If that entry is removed, the lockscreen is no longer displayed and the app is no longer locked. All local users are able to modify that file.	2021-02-05	2.1	CVE-2020-10553 MISC
qa-themes -- q2a_ultimate_seo	Question2Answer Q2A Ultimate SEO Version 1.3 is affected by cross-site scripting (XSS), which may lead to arbitrary remote code execution.	2021-02-05	3.5	CVE-2021-3258 MISC MISC MISC
roundcube -- roundcube	Roundcube before 1.4.11 allows XSS via crafted Cascading Style Sheets	2021-02-09	3.5	CVE-2021-26925

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CSS) token sequences during HTML email rendering.			CONFIRM MISC
secomea -- gatemanager_8250_firmware	A vulnerability in web UI input field of GateManager allows authenticated attacker to enter script tags that could cause XSS. This issue affects: GateManager all versions prior to 9.3.	2021-02-08	3.5	CVE-2020-29021 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of RAS files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12283)	2021-02-09	2.1	CVE-2020-28394 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of HPG files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12207)	2021-02-09	3.6	CVE-2020-27007 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PLT files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12209)	2021-02-09	3.6	CVE-2020-27008 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of CGM files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12163)	2021-02-09	3.6	CVE-2020-27004 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information. (ZDI-CAN-12040)	2021-02-09	2.1	CVE-2020-26998 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information. (ZDI-CAN-12042)	2021-02-09	2.1	CVE-2020-26999 MISC
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12043)	2021-02-09	3.6	CVE-2020-27002 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- scalance_w780_firmware	A vulnerability has been identified in SCALANCE W780 and W740 (IEEE 802.11n) family (All versions < V6.3). Sending specially crafted packets through the ARP protocol to an affected device could cause a partial denial-of-service, preventing the device to operate normally for a short period of time.	2021-02-09	3.3	CVE-2021-25666 MISC MISC
siemens -- simatic_pcs_7	A vulnerability has been identified in SIMATIC PCS 7 (All versions), SIMATIC WinCC (All versions < V7.5 SP2). Due to an insecure password verification process, an attacker could bypass the password protection set on protected files, thus being granted access to the protected content, circumventing authentication.	2021-02-09	2.1	CVE-2020-10048 MISC
smartfoxserver -- smartfoxserver	An issue was discovered in SmartFoxServer 2.17.0. Cleartext password disclosure can occur via /config/server.xml.	2021-02-09	2.1	CVE-2021-26550 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
telegram -- telegram	Telegram before 7.4 (212543) Stable on macOS stores the local passcode in cleartext, leading to information disclosure.	2021-02-12	2.1	CVE-2021-27204 MISC MISC
telegram -- telegram	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.	2021-02-12	2.1	CVE-2021-27205 MISC MISC
tufin -- securetrack	Username enumeration in present in Tufin SecureTrack. It's affecting all versions of SecureTrack. The vendor has decided not to fix this vulnerability. Vendor's response: "This attack requires access to the internal network. If an attacker is part of the internal network, they do not require access to TOS to know the usernames".	2021-02-09	3.3	CVE-2020-13461 MISC