Vulnerability Summary for the Week of January 25, 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
async-git_project -- async-git	The async-git package before 1.13.2 for Node.js allows OS Command Injection via shell metacharacters, as demonstrated by git.reset and git.tag.	2021-01-26	7.5	CVE-2021-3190 MISC MISC MISC CONFIRM
caret -- caret	A specially crafted Markdown document could cause the execution of malicious JavaScript code in Caret Editor before 4.0.0-rc22.	2021-01-26	10	CVE-2020-20269 MISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability.	2021-01-29	7.2	CVE-2021-25129 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow	2021-01-29	7.2	CVE-2021-25137 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in spx_restservice startflash_func function.			
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function.	2021-01-29	7.2	CVE-2021-25136 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function.	2021-01-29	7.2	CVE-2021-25135 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function.	2021-01-29	7.2	CVE-2021-25134 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function.	2021-01-29	7.2	CVE-2021-25133 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE	2021-01-29	7.2	CVE-2021-25132 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function.			
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function.	2021-01-29	7.2	CVE-2021-25131 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100	2021-01-29	7.2	CVE-2021-25130 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function.			
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability.	2021-01-29	7.2	CVE-2021-25128 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow	2021-01-29	7.2	CVE-2021-25127 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in spx_restservice generatesslcertificate_func function.			
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function.	2021-01-29	7.2	CVE-2021-25126 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability.	2021-01-29	7.2	CVE-2021-25125 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability.	2021-01-29	7.2	CVE-2021-25124 MISC
hpe -- cloudline_cl3100_gen10_server_firmware	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function.	2021-01-29	7.2	CVE-2021-25138 MISC
ibm -- security_guardium	IBM Security Guardium 11.2 could allow an authenticated user to gain	2021-01-27	9	CVE-2020-4952

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	root access due to improper access control. IBM X-Force ID: 192028.			XF CONFIRM
mingsoft -- mcms	An issue was discovered in ming-soft MCMS v5.0, where a malicious user can exploit SQL injection without logging in through /mcms/view.do.	2021-01-26	7.5	CVE-2020-23262 MISC
pepperl-fuchs -- io-link_master_4-eip_firmware	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to an authenticated blind OS Command Injection.	2021-01-22	9	CVE-2020-12513 CONFIRM
pyres -- termod4	Remote code execution in Pyrescom Termod4 time management devices before 10.04k allows authenticated remote attackers to arbitrary commands as root on the devices.	2021-01-26	9	CVE-2020-23160 MISC MISC
spotweb_project -- spotweb	SQL injection exists in Spotweb 1.4.9 because the notAllowedCommands protection mechanism is inadequate, e.g., a variation of the payload may be	2021-01-26	7.5	CVE-2021-3286 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	used. NOTE: this issue exists because of an incomplete fix for CVE-2020-35545.			

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- java_chassis	When handler-router component is enabled in servicecomb-java-chassis, authenticated user may inject some data and cause arbitrary code execution. The problem happens in versions between 2.0.0 ~ 2.1.3 and fixed in Apache ServiceComb-Java-Chassis 2.1.5	2021-01-25	6	CVE-2020-17532 CONFIRM CONFIRM
apache -- traffic_control	When ORT (now via atstccfg) generates ip_allow.config files in Apache Traffic Control 3.0.0 to 3.1.0	2021-01-26	5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and 4.0.0 to 4.1.0, those files include permissions that allow bad actors to push arbitrary content into and remove arbitrary content from CDN cache servers. Additionally, these permissions are potentially extended to IP addresses outside the desired range, resulting in them being granted to clients possibly outside the CDN arcitechture.			17522 MISC
deltaww -- tpeditor	TPEditor (v1.98 and prior) is vulnerable to two out-of-bounds write instances in the way it processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	2021-01-26	6.8	CVE-2020-27284 MISC
deltaww -- tpeditor	An untrusted pointer dereference has been identified in the way TPEditor(v1.98 and prior) processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	2021-01-26	6.8	CVE-2020-27288 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dzzoffice -- dzzoffice	attach/ajax.php in DzzOffice through 2.02.1 allows XSS via the editorid parameter.	2021-01-27	4.3	CVE-2021-3318 MISC
faststone -- image_viewer	FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0xbe9c4.	2021-01-26	6.8	CVE-2020-35844 MISC MISC
faststone -- image_viewer	FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0x96cf.	2021-01-26	6.8	CVE-2020-35845 MISC MISC
faststone -- image_viewer	FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0x956e.	2021-01-26	4.3	CVE-2020-35843 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
feehi -- feehi_cms	Feehi CMS 2.0.8 is affected by a cross-site scripting (XSS) vulnerability. When the user name is inserted as JavaScript code, browsing the post will trigger the XSS.	2021-01-26	4.3	CVE-2020-21146 MISC
feehi -- feehi_cms	Feehi CMS 2.1.0 is affected by an arbitrary file upload vulnerability, potentially resulting in remote code execution. After an administrator logs in, open the administrator image upload page to potentially upload malicious files.	2021-01-26	6.5	CVE-2020-22643 MISC
fujielectric -- v-server	Multiple out-of-bounds write issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	2021-01-27	6.8	CVE-2021-22653 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fujielectric -- v-server	Multiple out-of-bounds read issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	2021-01-27	6.8	CVE-2021-22655 MISC
fujielectric -- v-server	A heap-based buffer overflow issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	2021-01-27	6.8	CVE-2021-22641 MISC MISC
fujielectric -- v-server	An uninitialized pointer issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-	2021-01-27	6.8	CVE-2021-22639 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Simulator and V-Server Lite (versions prior to 4.0.10.0).			
fujielectric -- v-server	Multiple stack-based buffer overflow issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	2021-01-27	6.8	CVE-2021-22637 MISC MISC
google -- android	In A2DP_GetCodecType of a2dp_codec_config, there is a possible out-of-bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android, Versions: Android-10, Android ID: A-79703353.	2021-01-26	5	CVE-2020-0236 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hyweb -- hycms-j1	Hyweb HyCMS-J1's API fail to filter POST request parameters. Remote attackers can inject SQL syntax and execute commands without privilege.	2021-01-22	6.5	CVE-2021-22847 CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0 could allow a remote user to obtain sensitive information from HTTP response headers that could be used in further attacks against the system.	2021-01-27	5	CVE-2020-4815 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.3.0.1 and 1.4.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 185369.	2021-01-27	5	CVE-2020-4628 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0 could allow a remote attacker	2021-01-27	4.3	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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: 189703.			4816 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2021-01-27	4.3	CVE-2020-4820 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.3.0.1 could disclose sensitive information through HTTP headers which could be used in further attacks against the system. IBM X-Force ID: 192425.	2021-01-27	4	CVE-2020-4967 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- mq_internet_pass-thru	IBM MQ Internet Pass-Thru 2.1 and 9.2 could allow a remote user to cause a denial of service by sending malformed MQ data requests which would consume all available resources. IBM X-Force ID: 188093.	2021-01-22	5	CVE-2020-4766 XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 11.2 discloses sensitive information in the response headers that could be used in further attacks against the system. IBM X-Force ID: 174850.	2021-01-27	4	CVE-2020-4189 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: 192025.	2021-01-26	6.4	CVE-2020-4949 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iris -- star_practice_management	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access details about jobs he should not have access to via the Audit Trail Feature.	2021-01-29	4	CVE-2020-28406 MISC MISC
iris -- star_practice_management	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access the Billing page without the appropriate privileges.	2021-01-29	4	CVE-2020-28404 MISC MISC
iris -- star_practice_management	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access WIP details about jobs he should not have access to.	2021-01-29	4	CVE-2020-28401 MISC MISC
iris -- star_practice_management	An improper authorization vulnerability exists in Star Practice	2021-01-29	6.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Management Web version 2019.2.0.6, allowing an unauthorized user to change the privileges of any user of the application. This can be used to grant himself the administrative role or remove all administrative accounts of the application.			28405 MISC MISC
iris -- star_practice_management	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access Launcher Configuration Panel.	2021-01-29	6.5	CVE-2020-28402 MISC MISC
iris -- star_practice_management	A Cross-Site Request Forgery (CSRF) vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an attacker to change the privileges of any user of the application. This can be used to grant himself administrative role or remove the administrative account of the application.	2021-01-29	6.8	CVE-2020-28403 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jquery -- jquery_ui	This affects all versions of package jquery-ui; all versions of package org.fujion.webjars:jquery-ui. When the "dialog" is injected into an HTML tag more than once, the browser and the application may crash.	2021-01-22	5	CVE-2020-28488 MISC CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
mantisbt -- mantisbt	An issue was discovered in MantisBT before 2.24.4. Due to insufficient access-level checks, any logged-in user allowed to perform Group Actions can get access to the Summary fields of private Issues via	2021-01-29	4	CVE-2020-29605 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bug_arr[]= in a crafted bug_actiongroup_page.php URL. (The target Issues can have Private view status, or belong to a private Project.)			
mantisbt -- mantisbt	An issue was discovered in MantisBT before 2.24.4. A missing access check in bug_actiongroup.php allows an attacker (with rights to create new issues) to use the COPY group action to create a clone, including all bugnotes and attachments, of any private issue (i.e., one having Private view status, or belonging to a private Project) via the bug_arr[] parameter. This provides full access to potentially confidential information.	2021-01-29	4	CVE-2020-29604 MISC MISC
mantisbt -- mantisbt	In manage_proj_edit_page.php in MantisBT before 2.24.4, any unprivileged logged-in user can retrieve Private Projects' names via the manage_proj_edit_page.php	2021-01-29	4	CVE-2020-29603 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	project_id parameter, without having access to them.			
misp -- misp	A cross-site scripting (XSS) vulnerability exists in MISP v2.4.128 in app/Controller/UserSettingsController.php at SetHomePage() function. Due to a lack of controller validation in "path" parameter, an attacker can execute malicious JavaScript code.	2021-01-26	4.3	CVE-2020-24085 MISC
newbee-mall_project -- newbee-mall	newbee-mall 1.0 is affected by cross-site scripting in shop-cart/settle. Users only need to write xss payload in their address information when buying goods, which is triggered when viewing the "View Recipient Information" of this order in "Order Management Office".	2021-01-26	4.3	CVE-2020-23447 MISC
nodered -- node-red-dashboard	Node-RED-Dashboard before 2.26.2 allows ui_base/js/..%2f directory traversal to read files.	2021-01-26	5	CVE-2021-3223

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC CONFIRM
openldap -- openldap	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Certificate List Exact Assertion processing, resulting in denial of service.	2021-01-26	5	CVE-2020-36228 MISC MISC MISC
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading in an assertion failure in slapd in the X.509 DN parsing in decode.c ber_next_element, resulting in denial of service.	2021-01-26	5	CVE-2020-36230 MISC MISC MISC
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading to a memch->bv_len miscalculation and slapd crash in the saslAuthzTo processing, resulting in denial of service.	2021-01-26	5	CVE-2020-36226 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC
openldap -- openldap	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to slapd crashes in the Certificate Exact Assertion processing, resulting in denial of service (schema_init.c serialNumberAndIssuerCheck).	2021-01-26	5	CVE-2020-36221 MISC MISC MISC MISC MISC
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the saslAuthzTo validation, resulting in denial of service.	2021-01-26	5	CVE-2020-36222 MISC MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control handling, resulting in denial of service (double free and out-of-bounds read).	2021-01-26	5	CVE-2020-36223 MISC MISC MISC
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading to an invalid pointer free and slapd crash in the saslAuthzTo processing, resulting in denial of service.	2021-01-26	5	CVE-2020-36224 MISC MISC MISC MISC MISC MISC
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzTo processing, resulting in denial of service.	2021-01-26	5	CVE-2020-36225 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
openldap -- openldap	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 leading to a slapd crash in the X.509 DN parsing in ad_keystring, resulting in denial of service.	2021-01-26	5	CVE-2020-36229 MISC MISC MISC
openldap -- openldap	A flaw was discovered in OpenLDAP before 2.4.57 leading to an infinite loop in slapd with the cancel_extop Cancel operation, resulting in denial of service.	2021-01-26	5	CVE-2020-36227 MISC MISC MISC
panasonic -- fpwin_pro	FPWIN Pro is vulnerable to an out-of-bounds read vulnerability when a user opens a maliciously crafted project file, which may allow an attacker to remotely execute arbitrary code.	2021-01-26	6.8	CVE-2020-16236 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pepperl-fuchs -- io-link_master_4-eip_firmware	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to a NULL Pointer Dereference that leads to a DoS in discoveryd	2021-01-22	4	CVE-2020-12514 CONFIRM
pepperl-fuchs -- io-link_master_4-eip_firmware	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to a Cross-Site Request Forgery (CSRF) in the web interface.	2021-01-22	6.8	CVE-2020-12511 CONFIRM
phpgurukul -- daily_expense_tracker_system	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the user-profile.php Full Name field.	2021-01-29	4.3	CVE-2021-26303 MISC
phpgurukul_daily_expense_tracker_system_project -- phpgurukul_daily_expense_tracker_system	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the add-expense.php Item parameter.	2021-01-29	4.3	CVE-2021-26304 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
report_project -- report	The MediaWiki "Report" extension has a Cross-Site Request Forgery (CSRF) vulnerability. Before fixed version, there was no protection against CSRF checks on Special:Report, so requests to report a revision could be forged. The problem has been fixed in commit f828dc6 by making use of MediaWiki edit tokens.	2021-01-25	4.3	CVE-2021-21275 MISC CONFIRM
revive-adserver -- revive_adserver	Revive Adserver before 5.1.1 is vulnerable to a reflected XSS vulnerability in stats.php via the `setPerPage` parameter.	2021-01-28	4.3	CVE-2021-22875 MISC MISC MISC
revive-adserver -- revive_adserver	Revive Adserver before 5.1.1 is vulnerable to a reflected XSS vulnerability in userlog-index.php via the `period_preset` parameter.	2021-01-28	4.3	CVE-2021-22874 MISC MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apfell_project -- apfell	APfell 1.4 is vulnerable to authenticated reflected cross-site scripting (XSS) in /apiui/command_ through the payloadtypes_callback function, which allows an attacker to steal remote admin/user session and/or adding new users to the administration panel.	2021-01-26	3.5	CVE-2020-23014 MISC MISC
bdtask -- multi-store	Stored XSS vulnerability in BDTASK Multi-Store Inventory Management System 1.0 allows a local admin to inject arbitrary code via the Customer Name Field.	2021-01-27	3.5	CVE-2020-36012 MISC MISC MISC
bigprof -- online_invoicing_system	Online Invoicing System (OIS) is open source software which is a lean invoicing system for small businesses, consultants and freelancers created using AppGini. In OIS version 4.0 there is a stored XSS which can enables an attacker takeover of the admin account through a payload that extracts a csrf token and sends a request to change password. It	2021-01-22	3.5	CVE-2021-21260 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	has been found that Item description is reflected without sanitization in app/items_view.php which enables the malicious scenario.			
compo -- composr_cms	Composr CMS 10.0.34 is affected by cross-site scripting (XSS) which allows remote attackers to inject an arbitrary web script or HTML via Add Banners in the Description field.	2021-01-26	3.5	CVE-2020-35310 MISC
hyweb -- hycms-j1	Hyweb HyCMS-J1 backend editing function does not filter special characters. Users after log-in can inject JavaScript syntax to perform a stored XSS (Stored Cross-site scripting) attack.	2021-01-22	3.5	CVE-2021-22849 CONFIRM
ibm -- collaborative_lifecycle_management	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182434.	2021-01-27	3.5	CVE-2020-4524 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- collaborative_lifecycle_management	IBM Jazz Foundation products could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 183315.	2021-01-27	3.5	CVE-2020-4547 XF CONFIRM
ibm -- collaborative_lifecycle_management	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 190457.	2021-01-27	3.5	CVE-2020-4855 XF CONFIRM
ibm -- collaborative_lifecycle_management	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 190741.	2021-01-27	3.5	CVE-2020-4865 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- collaborative_lifecycle_management	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963.	2021-01-27	3.5	CVE-2021-20357 XF CONFIRM
ibm -- spectrum_scale	IBM Spectrum Scale 5.0.0 through 5.0.5.4 and 5.1.0 could allow a local user to poison log files which could impact support and development efforts. IBM X-Force ID: 190971.	2021-01-26	2.1	CVE-2020-4889 XF CONFIRM
o-dyn -- collabtive	Collabtive 3.1 allows XSS when an authenticated user enters an XSS payload into the address section of the profile edit page, aka the manageuser.php?action=edit address1 parameter.	2021-01-29	3.5	CVE-2021-3298 MISC MISC
openwrt -- openwrt	LuCI in OpenWrt 18.06.0 through 18.06.4 allows stored XSS via a crafted SSID.	2021-01-26	3.5	CVE-2019-25015 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pepperl-fuchs -- io-link_master_4-eip_firmware	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to an authenticated reflected POST Cross-Site Scripting	2021-01-22	3.5	CVE-2020-12512 CONFIRM
rockoa -- rockoa	RockOA V1.9.8 is affected by a cross-site scripting (XSS) vulnerability which allows remote attackers to send malicious code to the administrator and execute JavaScript code, because webmain/flow/input/mode_emailmAction.php does not perform strict filtering.	2021-01-26	3.5	CVE-2020-21147 MISC MISC

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rocket.chat -- rocket.chat	Rocket.Chat server before 3.9.0 is vulnerable to a self cross-site scripting (XSS) vulnerability via the drag & drop functionality in message boxes.	2021-01-26	not yet calculated	CVE-2020-8292 MISC MISC
4images -- image_gallary_management_system	4images Image Gallery Management System 1.7.11 is affected by cross-site scripting (XSS) in the Image URL. This vulnerability can result in an attacker to inject the XSS payload into the IMAGE URL. Each time a user visits that URL, the XSS triggers and the attacker can be able to steal the cookie according to the crafted payload.	2021-01-26	not yet calculated	CVE-2020-35853 MISC
abi_stable -- abi_stable	An issue was discovered in the abi_stable crate before 0.9.1 for Rust. DrainFilter lacks soundness because of a double drop.	2021-01-26	not yet calculated	CVE-2020-36212 MISC
abi_stable -- abi_stable	An issue was discovered in the abi_stable crate before 0.9.1 for Rust. A retain call can create an invalid UTF-8 string, violating soundness.	2021-01-26	not yet calculated	CVE-2020-36213 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accfly -- wireless_security_ir_camera_720p	An issue was discovered on Accfly Wireless Security IR Camera System 720P with software versions v3.10.73 through v4.15.77. There is an unauthenticated heap-based buffer overflow in the function CNetClientTalk::OprMsg during incoming message handling.	2021-01-28	not yet calculated	CVE-2020-25783 MISC
accfly -- wireless_security_ir_camera_720p	An issue was discovered on Accfly Wireless Security IR Camera System 720P with software versions v3.10.73 through v4.15.77. There is an unauthenticated stack-based buffer overflow in the function CFtpProtocol::FtpLogin during the update procedure.	2021-01-28	not yet calculated	CVE-2020-25785 MISC
accfly -- wireless_security_ir_camera_720p	An issue was discovered on Accfly Wireless Security IR Camera 720P System with software versions v3.10.73 through v4.15.77. There is an unauthenticated stack-based buffer overflow in the function CNetClientManage::ServerIP_Proto_Set during incoming message handling.	2021-01-28	not yet calculated	CVE-2020-25782 MISC
accfly -- wireless_security_ir_camera_720p	An issue was discovered on Accfly Wireless Security IR Camera System 720P with software versions v3.10.73 through v4.15.77. There is an	2021-01-28	not yet calculated	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated stack-based buffer overflow in the function CNetClientGuard::SubOprMsg during incoming message handling.			25784 MISC
acdsee -- professional_2021	PlugIns\IDE_ACDStd.apl in ACDSee Professional 2021 14.0 1721 has a User Mode Write Access Violation starting at IDE_ACDStd!JPEGTransW+0x000000000000c7f4 via a crafted BMP image.	2021-01-26	not yet calculated	CVE-2021-26026 MISC
acdsee -- professional_2021	PlugIns\IDE_ACDStd.apl in ACDSee Professional 2021 14.0 1721 has a User Mode Write Access Violation starting at IDE_ACDStd!zlibVersion+0x0000000000004e5e via a crafted BMP image.	2021-01-26	not yet calculated	CVE-2021-26025 MISC
acronis_true_image -- acronis_true_image	Acronis True Image for Windows prior to 2021 Update 3 allowed local privilege escalation due to a DLL hijacking vulnerability in multiple components, aka an Untrusted Search Path issue.	2021-01-29	not yet calculated	CVE-2020-35145 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aovec -- aovec	An issue was discovered in the aovec crate through 2020-12-10 for Rust. Because Aovec<T> does not have bounds on its Send trait or Sync trait, a data race and memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36207 MISC
apache -- activemq_artemis	The optional ActiveMQ LDAP login module can be configured to use anonymous access to the LDAP server. In this case, for Apache ActiveMQ Artemis prior to version 2.16.0 and Apache ActiveMQ prior to versions 5.16.1 and 5.15.14, the anonymous context is used to verify a valid users password in error, resulting in no check on the password.	2021-01-27	not yet calculated	CVE-2021-26117 MLIST MLIST MISC
apache -- activemq_artemis	While investigating ARTEMIS-2964 it was found that the creation of advisory messages in the OpenWire protocol head of Apache ActiveMQ Artemis 2.15.0 bypassed policy based access control for the entire session. Production of advisory messages was not subject to access control in error.	2021-01-27	not yet calculated	CVE-2021-26118 MLIST MISC
apache -- druid	Apache Druid includes the ability to execute user-provided JavaScript code embedded in various types of requests. This functionality is intended for use in high-trust environments, and is disabled by default.	2021-01-29	not yet calculated	CVE-2021-25646 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	However, in Druid 0.20.0 and earlier, it is possible for an authenticated user to send a specially-crafted request that forces Druid to run user-provided JavaScript code for that request, regardless of server configuration. This can be leveraged to execute code on the target machine with the privileges of the Druid server process.			MLIST MLIST MLIST MISC
apache -- hadoop	In Apache Hadoop 3.2.0 to 3.2.1, 3.0.0-alpha1 to 3.1.3, and 2.0.0-alpha to 2.10.0, WebHDFS client might send SPNEGO authorization header to remote URL without proper verification.	2021-01-26	not yet calculated	CVE-2020-9492 MISC MLIST
archer -- archer	Archer before 6.8 P2 (6.8.0.2) is affected by a path exposure vulnerability. A remote authenticated malicious attacker with access to service files may obtain sensitive information to use it in further attacks.	2021-01-29	not yet calculated	CVE-2020-29536 CONFIRM MISC
archer -- archer	Archer before 6.8 P2 (6.8.0.2) is affected by an open redirect vulnerability. A remote privileged attacker may potentially redirect legitimate users to arbitrary	2021-01-29	not yet calculated	CVE-2020-29537

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	web sites and conduct phishing attacks. The attacker could then steal the victims' credentials and silently authenticate them to the Archer application without the victims realizing an attack occurred.			CONFIRM MISC
archer -- archer	Archer before 6.9 P1 (6.9.0.1) contains an improper access control vulnerability in an API. A remote authenticated malicious administrative user can potentially exploit this vulnerability to gather information about the system, and may use this information in subsequent attacks.	2021-01-29	not yet calculated	CVE-2020-29538 CONFIRM MISC
archer -- archer	Archer before 6.8 P4 (6.8.0.4) contains a stored XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When application users access the corrupted data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2021-01-29	not yet calculated	CVE-2020-29535 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
assuweb -- assuweb	Deserialization of untrusted data in the login page of ASSUWEB 359.3 build 1 subcomponent of ACA ASSUREX RENTES product allows a remote attacker to inject unsecure serialized Java object using a specially crafted HTTP request, resulting in an unauthenticated remote code execution on the server.	2021-01-28	not yet calculated	CVE-2021-3160 MISC MISC
async-h1 -- async-h1	An issue was discovered in the async-h1 crate before 2.3.0 for Rust. Request smuggling can occur when used behind a reverse proxy.	2021-01-26	not yet calculated	CVE-2020-36202 MISC
aterm -- wf800hp_firmware	Cross-site scripting vulnerability in Aterm WF800HP firmware Ver1.0.9 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-01-28	not yet calculated	CVE-2021-20620 MISC MISC MISC
aterm -- wg2600hp_firmware	Cross-site request forgery (CSRF) vulnerability in Aterm WG2600HP firmware Ver1.0.2 and earlier, and Aterm WG2600HP2 firmware Ver1.0.2 and earlier allows remote attackers to hijack the	2021-01-28	not yet calculated	CVE-2021-20621 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication of administrators via unspecified vectors.			MISC MISC
aterm -- wg2600hp_firmware	Cross-site scripting vulnerability in Aterm WG2600HP firmware Ver1.0.2 and earlier, and Aterm WG2600HP2 firmware Ver1.0.2 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-01-28	not yet calculated	CVE-2021-20622 MISC MISC MISC
atlassian -- bamboo	Affected versions of Atlassian Bamboo allow an unauthenticated remote attacker to view a stack trace that may reveal the path for the home directory in disk and if certain files exists on the tmp directory, via a Sensitive Data Exposure vulnerability in the /chart endpoint. The affected versions are before version 7.2.2.	2021-01-28	not yet calculated	CVE-2021-26067 MISC
atomic-option -- atomic-option	An issue was discovered in the atomic-option crate through 2020-10-31 for Rust. Because AtomicOption<T> implements Sync unconditionally, a data race can occur.	2021-01-26	not yet calculated	CVE-2020-36219 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autoand -- autoand	An issue was discovered in the autorand crate before 0.2.3 for Rust. Because of impl Random on arrays, uninitialized memory can be dropped when a panic occurs, leading to memory corruption.	2021-01-26	not yet calculated	CVE-2020-36210 MISC
av-data -- av-data	An issue was discovered in the av-data crate before 0.3.0 for Rust. A raw pointer is dereferenced, leading to a read of an arbitrary memory address, sometimes causing a segfault.	2021-01-26	not yet calculated	CVE-2021-25904 MISC
bakeshop -- online_ordering_system	Bakeshop Online Ordering System in PHP/MySQLi 1.0 is affected by cross-site scripting (XSS) which allows remote attackers to inject an arbitrary web script or HTML in admin dashboard - "Categories".	2021-01-26	not yet calculated	CVE-2020-35309 MISC
basic_dsp_matrix -- basic_dsp_matrix	An issue was discovered in the basic_dsp_matrix crate before 0.9.2 for Rust. When a TransformContent panic occurs, a double drop can be performed.	2021-01-26	not yet calculated	CVE-2021-25906 MISC
bitcoin -- core	bitcoind in Bitcoin Core through 0.21.0 can create a new file in an arbitrary directory (e.g., outside the ~/.bitcoin directory) via a dumpwallet RPC call.	2021-01-26	not yet calculated	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				3195 MISC
bosch -- fsm-2500_server_and_fsm-5000_server	Use of Hard-coded Credentials in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows an unauthenticated remote attacker to log into the database with admin-privileges. This may result in complete compromise of the confidentiality and integrity of the stored data as well as a high availability impact on the database itself. In addition, an attacker may execute arbitrary commands on the underlying operating system.	2021-01-26	not yet calculated	CVE-2020-6779 MISC
bosch -- fsm-2500_server_and_fsm-5000_server	Use of Password Hash With Insufficient Computational Effort in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows a remote attacker with admin privileges to dump the credentials of other users and possibly recover their plain-text passwords by brute-forcing the MD5 hash.	2021-01-26	not yet calculated	CVE-2020-6780 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bra -- bra	An issue was discovered in the bra crate before 0.1.1 for Rust. It lacks soundness because it can read uninitialized memory.	2021-01-26	not yet calculated	CVE-2021-25905 MISC
buttplug -- buttplug	An issue was discovered in the buttplug crate before 1.0.4 for Rust. ButtplugFutureStateShared does not properly consider (!Send|!Sync) objects, leading to a data race.	2021-01-26	not yet calculated	CVE-2020-36218 MISC
cache -- cache	An issue was discovered in the cache crate through 2021-01-01 for Rust. A raw pointer is dereferenced.	2021-01-26	not yet calculated	CVE-2021-25903 MISC
cakephp -- cakephp	A vulnerability exists in CakePHP versions 4.0.x through 4.1.3. The CsrfProtectionMiddleware component allows method override parameters to bypass CSRF checks by changing the HTTP request method to an arbitrary string that is not in the list of request methods that CakePHP checks. Additionally, the route middleware does not verify that this overriden method (which can be an arbitrary string) is actually an HTTP method.	2021-01-26	not yet calculated	CVE-2020-35239 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cdr-rs -- cdr-rs	An issue was discovered in Deserializer::read_vec in the cdr crate before 0.2.4 for Rust. A user-provided Read implementation can gain access to the old contents of newly allocated heap memory, violating soundness.	2021-01-29	not yet calculated	CVE-2021-26305 MISC
churchrota -- churchrota	ChurchRota 2.6.4 is vulnerable to authenticated remote code execution. The user does not need to have file upload permission in order to upload and execute an arbitrary file via a POST request to resources.php.	2021-01-26	not yet calculated	CVE-2021-3164 MISC MISC
ckeditor -- ckeditor	It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted text into the Styles input of specific dialogs (in the Advanced Tab for Dialogs plugin).	2021-01-26	not yet calculated	CVE-2021-26271 MISC
ckeditor -- ckeditor	It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted URL-like text into the editor, and then press Enter or Space (in the Autolink plugin).	2021-01-26	not yet calculated	CVE-2021-26272 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ckeditor -- ckeditor	CKEditor 5 is an open source rich text editor framework with a modular architecture. The CKEditor 5 Markdown plugin (@ckeditor/ckeditor5-markdown-gfm) before version 25.0.0 has a regex denial of service (ReDoS) vulnerability. The vulnerability allowed to abuse link recognition regular expression, which could cause a significant performance drop resulting in browser tab freeze. It affects all users using CKEditor 5 Markdown plugin at version <= 24.0.0. The problem has been recognized and patched. The fix will be available in version 25.0.0.	2021-01-29	not yet calculated	CVE-2021-21254 MISC CONFIRM MISC
codiad -- codiad	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** Codiad 2.8.4 /componetns/user/class.user.php:Authenticate() is vulnerable in magic hash authentication bypass. If encrypted or hash value for the passwords form certain formats of magic hash, e.g, 0e123, another hash value 0e234 something can successfully authenticate.	2021-01-27	not yet calculated	CVE-2020-23355 MISC
conquer-once -- conquer-once	An issue was discovered in the conquer-once crate before 0.3.2 for Rust. Thread crossing can occur for	2021-01-26	not yet calculated	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a non-Send but Sync type, leading to memory corruption.			36208 MISC
containers -- containers	An issue was discovered in the containers crate before 0.9.11 for Rust. When a panic occurs, a util::{mutate,mutate2} double drop can be performed.	2021-01-26	not yet calculated	CVE-2021-25907 MISC
cpanel -- cpanel	cPanel before 92.0.9 allows a Reseller to bypass the suspension lock (SEC-578).	2021-01-26	not yet calculated	CVE-2021-26266 MISC
cpanel -- cpanel	cPanel before 92.0.9 allows a MySQL user (who has an old-style password hash) to bypass suspension (SEC-579).	2021-01-26	not yet calculated	CVE-2021-26267 MISC
d-link -- dir_825_r1_devices	An issue was discovered on D-Link DIR-825 R1 devices through 3.0.1 before 2020-11-20. A buffer overflow in the web interface allows attackers to achieve pre-authentication remote code execution.	2021-01-29	not yet calculated	CVE-2020-29557 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
delta_electronics -- ispsoft	A use after free issue has been identified in the way ISPSoft(v3.12 and prior) processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution.	2021-01-26	not yet calculated	CVE-2020-27280 MISC
dh2i -- dxenterprise_and_dxodyssey	A path traversal vulnerability in the DxWebEngine component of DH2i DxEnterprise and DxOdyssey for Windows, version 19.5 through 20.x before 20.0.219.0, allows an attacker to read any file on the host file system via an HTTP request.	2021-01-29	not yet calculated	CVE-2021-3341 MISC
duncaen -- opendoas	In OpenDoas from 6.6 to 6.8 the users PATH variable was incorrectly inherited by authenticated executions if the authenticating rule allowed the user to execute any command. Rules that only allowed to authenticated user to execute specific commands were not affected by this issue.	2021-01-28	not yet calculated	CVE-2019-25016 MISC MISC MISC MISC
ecostruxure -- operator_terminal_expert_and_pro-face_blue	A CWE-20: Improper Input Validation vulnerability exists in EcoStruxure™ Operator Terminal Expert and Pro-face BLUE (version details in the notification) that could cause arbitrary code	2021-01-26	not yet calculated	CVE-2020-28221 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution when the Ethernet Download feature is enable on the HMI.			
ecostruxure -- power_build	A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists in the EcoStruxure Power Build - Rapsody software (V2.1.13 and prior) that could allow a stack-based buffer overflow to occur which could result in remote code execution when a malicious SSD file is uploaded and improperly parsed.	2021-01-26	not yet calculated	CVE-2021-22698 MISC
ecostruxure -- power_build	A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists in the EcoStruxure Power Build - Rapsody software (V2.1.13 and prior) that could allow a use-after-free condition which could result in remote code execution when a malicious SSD file is uploaded and improperly parsed.	2021-01-26	not yet calculated	CVE-2021-22697 MISC
egavilan -- media_crud_operation	Stored Cross Site Scripting (XSS) vulnerability in EGavilan Media CRUD Operation with PHP, MySQL, Bootstrap, and Dompdf via First Name or Last Name parameter in the 'Add New Record Feature'.	2021-01-28	not yet calculated	CVE-2020-36115 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
egavilanmedia -- user_registration_and_login_system	EgavilanMedia User Registration & Login System 1.0 is affected by SQL injection to the admin panel, which may allow arbitrary code execution.	2021-01-26	not yet calculated	CVE-2020-35263 MISC
electron -- electron	The Electron framework lets you write cross-platform desktop applications using JavaScript, HTML and CSS. In affected versions of Electron IPC messages sent from the main process to a subframe in the renderer process, through webContents.sendToFrame, event.reply or when using the remote module, can in some cases be delivered to the wrong frame. If your app uses remote, calls webContents.sendToFrame, or calls event.reply in an IPC message handler then it is impacted by this issue. This has been fixed in versions 9.4.0, 10.2.0, 11.1.0, and 12.0.0-beta.9. There are no workarounds for this issue.	2021-01-28	not yet calculated	CVE-2020-26272 MISC MISC MISC CONFIRM MISC
eset -- multiple_products	A local (authenticated) low-privileged user can exploit a behavior in an ESET installer to achieve arbitrary file overwrite (deletion) of any file via a symlink, due to insecure permissions. The possibility of exploiting this vulnerability is limited and can only take place during the installation phase	2021-01-26	not yet calculated	CVE-2020-26941 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of ESET products. Furthermore, exploitation can only succeed when Self-Defense is disabled. Affected products are: ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium versions 13.2 and lower; ESET Endpoint Antivirus, ESET Endpoint Security, ESET NOD32 Antivirus Business Edition, ESET Smart Security Business Edition versions 7.3 and lower; ESET File Security for Microsoft Windows Server, ESET Mail Security for Microsoft Exchange Server, ESET Mail Security for IBM Domino, ESET Security for Kerio, ESET Security for Microsoft SharePoint Server versions 7.2 and lower.			
eventio -- eventio	An issue was discovered in Input<R> in the eventio crate before 0.5.1 for Rust. Because a non-Send type can be sent to a different thread, a data race and memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36216 MISC
fil-ocl -- fil-ocl	An issue was discovered in the fil-ocl crate through 2021-01-04 for Rust. From<EventList> can lead to a double free.	2021-01-26	not yet calculated	CVE-2021-25908 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flarum -- flarum	Flarum is an open source discussion platform for websites. The "Flarum Sticky" extension versions 0.1.0-beta.14 and 0.1.0-beta.15 has a cross-site scripting vulnerability. A change in release beta 14 of the Sticky extension caused the plain text content of the first post of a pinned discussion to be injected as HTML on the discussion list. The issue was discovered following an internal audit. Any HTML would be injected through the m.trust() helper. This resulted in an HTML injection where <script> tags would not be executed. However it was possible to run javascript from other HTML attributes, enabling a cross-site scripting (XSS) attack to be performed. Since the exploit only happens with the first post of a pinned discussion, an attacker would need the ability to pin their own discussion, or be able to edit a discussion that was previously pinned. On forums where all pinned posts are authored by your staff, you can be relatively certain the vulnerability has not been exploited. Forums where some user-created discussions were pinned can look at the first post edit date to find whether the vulnerability might have been exploited. Because Flarum doesn't store the post content history, you cannot be certain if a malicious edit was reverted. The fix will be available in version v0.1.0-beta.16 with Flarum beta	2021-01-26	not yet calculated	CVE-2021-21283 MISC MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	16. The fix has already been back-ported to Flarum beta 15 as version v0.1.0-beta.15.1 of the Sticky extension. Forum administrators can disable the Sticky extension until they are able to apply the update. The vulnerability cannot be exploited while the extension is disabled.			
foris -- foris	Foris before 101.1.1, as used in Turris OS, lacks certain HTML escaping in the login template.	2021-01-29	not yet calculated	CVE-2021-3346 MISC MISC MISC
ftpd -- ftpd	The ftpd gem 0.2.1 for Ruby allows remote attackers to execute arbitrary OS commands via shell metacharacters in a LIST or NLST command argument within FTP protocol traffic.	2021-01-26	not yet calculated	CVE-2013-2512 MISC
geeni -- gnc-cw013	An issue was discovered on Geeni GNC-CW013 doorbell 1.8.1 devices. A vulnerability exists in the Telnet service that allows a remote attacker to take full control of the device with a high-privileged	2021-01-26	not yet calculated	CVE-2020-28998 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	account. The vulnerability exists because a system account has a default and static password.			
geeni -- gnc-cw013	An issue was discovered in Apexis Streaming Video Web Application on Geeni GNC-CW013 doorbell 1.8.1 devices. A remote attacker can take full control of the camera with a high-privileged account. The vulnerability exists because a static username and password are compiled into a shared library (libhipcam.so) used to provide the streaming camera service.	2021-01-26	not yet calculated	CVE-2020-28999 MISC MISC
geeni -- gnc-cw013	An issue was discovered on Geeni GNC-CW013 doorbell 1.8.1 devices. A vulnerability exists in the RTSP service that allows a remote attacker to take full control of the device with a high-privileged account. By sending a crafted message, an attacker is able to remotely deliver a telnet session. Any attacker that has the ability to control DNS can exploit this vulnerability to remotely login to the device and gain access to the camera system.	2021-01-26	not yet calculated	CVE-2020-29000 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
geeni -- mulitple_products	An issue was discovered on Geeni GNC-CW028 Camera 2.7.2, Geeni GNC-CW025 Doorbell 2.9.5, Merkury MI-CW024 Doorbell 2.9.6, and Merkury MI-CW017 Camera 2.9.6 devices. A vulnerability exists in the RESTful Services API that allows a remote attacker to take full control of the camera with a high-privileged account. The vulnerability exists because a static username and password are compiled into the ppsapp RESTful application.	2021-01-26	not yet calculated	CVE-2020-29001 MISC MISC
gfwx -- gfwx	An issue was discovered in the gfwx crate before 0.3.0 for Rust. Because ImageChunkMut does not have bounds on its Send trait or Sync trait, a data race and memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36211 MISC
glsl-layout -- glsl-layout	An issue was discovered in the glsl-layout crate before 0.4.0 for Rust. When a panic occurs, map_array can perform a double drop.	2021-01-26	not yet calculated	CVE-2021-25902 MISC
gnu -- c_library	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding,	2021-01-27	not yet calculated	CVE-2021-3326 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.			MISC MISC
go -- go	Go before 1.14.14 and 1.15.x before 1.15.7 on Windows is vulnerable to Command Injection and remote code execution when using the "go get" command to fetch modules that make use of cgo (for example, cgo can execute a gcc program from an untrusted download).	2021-01-26	not yet calculated	CVE-2021-3115 CONFIRM CONFIRM
go -- go	In Go before 1.14.14 and 1.15.x before 1.15.7, crypto/elliptic/p224.go can generate incorrect outputs, related to an underflow of the lowest limb during the final complete reduction in the P-224 field.	2021-01-26	not yet calculated	CVE-2021-3114 CONFIRM CONFIRM
godaddy -- godaddy	** DISPUTED ** scripts/cli.js in the GoDaddy node-config-shield (aka Config Shield) package before 0.2.2 for Node.js calls eval when processing a set command. NOTE: the vendor reportedly states	2021-01-27	not yet calculated	CVE-2021-26276 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that this is not a vulnerability. The set command was not intended for use with untrusted data.			
google -- android	In checkGrantUriPermission of UriGrantsManagerService.java, there is a possible way to access contacts due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-138791358	2021-01-26	not yet calculated	CVE-2020-27098 MISC
google -- android	In checkGrantUriPermission of UriGrantsManagerService.java, there is a possible permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140729426	2021-01-26	not yet calculated	CVE-2020-27097 MISC
gstreamer -- h264	A flaw was found in the gstreamer h264 component of gst-plugins-bad before v1.18.1 where when parsing a h264 header, an attacker could cause the	2021-01-26	not yet calculated	CVE-2021-3185 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stack to be smashed, memory corruption and possibly code execution.			
hackolade -- hackolade	An elevation of privilege vulnerability exists in Hackolade versions prior 4.2.0 on Windows has an issue in specific deployment scenarios that could allow local users to gain elevated privileges during an uninstall of the application.	2021-01-26	not yet calculated	CVE-2020-25737 MISC
hashconsing -- hashconsing	An issue was discovered in the hashconsing crate before 1.1.0 for Rust. Because HConsed does not have bounds on its Send trait or Sync trait, memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36215 MISC
hedgedoc -- hedgedoc	HedgeDoc is open source software which lets you create real-time collaborative markdown notes. In HedgeDoc before version 1.7.2, an attacker can inject arbitrary JavaScript into a HedgeDoc note, which is executed when the note is viewed in slide mode. Depending on the configuration of the instance, the attacker may not need authentication to create or edit notes. The problem is patched in HedgeDoc 1.7.2. ### Workarounds Disallow loading JavaScript from 3rd party sites using the	2021-01-22	not yet calculated	CVE-2021-21259 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`Content-Security-Policy` header. Note that this will break some embedded content. ### References This issue was discovered by @TobiasHoll and reported to hackmdio/codimd: https://github.com/hackmdio/codimd/issues/1648 ### For more information If you have any questions or comments about this advisory: * Open an topic on our community forum * Join our matrix room			
hewlett_packard -- multiple_products	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice addlicense_func function.	2021-01-29	not yet calculated	CVE-2021-25123 MISC
hitachi -- vantara_pentaho	The New Analysis Report in Hitachi Vantara Pentaho through 7.x - 8.x contains a DOM-based Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Analysis Report Description' field in 'About this Report' section. Remediated in >= 8.3.0.9, >= 9.0.0.1, and >= 9.1.0.0 GA.	2021-01-29	not yet calculated	CVE-2020-24669 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hitachi -- vantara_pentaho	The Dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'type' attribute of 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, and >= 8.3.0.0 GA.	2021-01-29	not yet calculated	CVE-2020-24670 MISC MISC
hitachi -- vantara_pentaho	The Dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains an XML Entity Expansion injection vulnerability, which allows an authenticated remote users to trigger a denial of service (DoS) condition. Specifically, the vulnerability lies in the 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, >= 8.3.0.0 GA	2021-01-29	not yet calculated	CVE-2020-24665 MISC MISC
hitachi -- vantara_pentaho	The Analysis Report in Hitachi Vantara Pentaho through 7.x - 8.x contains a stored Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Display Name' parameter. Remediated in >= 9.1.0.1	2021-01-29	not yet calculated	CVE-2020-24666 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hitachi -- vantara_pentaho	The dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'pho:title' attribute of 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, and >= 8.3.0.0 GA.	2021-01-29	not yet calculated	CVE-2020-24664 MISC MISC
home_assistant -- home_assistant	** DISPUTED ** Home Assistant before 2021.1.3 does not have a protection layer that can help to prevent directory-traversal attacks against custom integrations. NOTE: the vendor's perspective is that the vulnerability itself is in custom integrations written by third parties, not in Home Assistant; however, Home Assistant does have a security update that is worthwhile in addressing this situation.	2021-01-26	not yet calculated	CVE-2021-3152 CONFIRM MISC
htcondor -- condor_credd	condor_credd in HTCondor before 8.9.11 allows Directory Traversal outside the SEC_CREDENTIAL_DIRECTORY_OAUTH directory, as demonstrated by creating a file under /etc that will later be executed by root.	2021-01-27	not yet calculated	CVE-2021-25311 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
htcondor -- htcondor	HTCondor before 8.9.11 allows a user to submit a job as another user on the system, because of a flaw in the IDTOKENS authentication method.	2021-01-27	not yet calculated	CVE-2021-25312 MISC
ibm -- infosphere_information_server	** UNSUPPORTED WHEN ASSIGNED ** IBM InfoSphere Information Server 8.5.0.0 is affected by deserialization of untrusted data which could allow remote unauthenticated attackers to execute arbitrary code. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-01-26	not yet calculated	CVE-2020-27583 MISC
ibm -- mq	IBM MQ 7.5, 8.0, 9.0, 9.1, 9.2 LTS, and 9.2 CD could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization of trusted data. An attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 186509.	2021-01-28	not yet calculated	CVE-2020-4682 XF CONFIRM
ibm -- qradar_siem	IBM QRadar SIEM 7.4.0 to 7.4.2 Patch 1 and 7.3.0 to 7.3.3 Patch 7 could allow a remote attacker to execute arbitrary commands on the system, caused by insecure deserialization of user-supplied content	2021-01-28	not yet calculated	CVE-2020-4888 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by the Java deserialization function. By sending a malicious serialized Java object, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 190912.			CONFIRM
ibm -- qradar_siem	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1, 7.4.0 to 7.4.1 Patch 1, and 7.3.0 to 7.3.3 Patch 5 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 189224.	2021-01-27	not yet calculated	CVE-2020-4787 XF CONFIRM
ibm -- qradar_siem	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1, 7.4.0 to 7.4.1 Patch 1, and 7.3.0 to 7.3.3 Patch 5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 189302.	2021-01-27	not yet calculated	CVE-2020-4789 XF CONFIRM
ibm -- qradar_siem	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1, 7.4.0 to 7.4.1 Patch 1, and 7.3.0 to 7.3.3 Patch 5 is vulnerable to server side request forgery (SSRF).	2021-01-27	not yet calculated	CVE-2020-4786

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 189221.			XF CONFIRM
ide_atapi_cmd_reply_end -- ide_atapi_cmd_reply_end	ide_atapi_cmd_reply_end in hw/ide/atapi.c in QEMU 5.1.0 allows out-of-bounds read access because a buffer index is not validated.	2021-01-26	not yet calculated	CVE-2020-29443 MISC MISC
im -- im	An issue was discovered in the im crate through 2020-11-09 for Rust. Because TreeFocus does not have bounds on its Send trait or Sync trait, a data race can occur.	2021-01-26	not yet calculated	CVE-2020-36204 MISC
iniparserjs -- iniparserjs	This affects all versions of package iniparserjs. This vulnerability relates when ini_parser.js is concentrating arrays. Depending on if user input is provided, an attacker can overwrite and pollute the object prototype of a program.	2021-01-29	not yet calculated	CVE-2021-23328 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
istio_pilot -- istio_pilot	A NULL pointer dereference was found in pkg/proxy/envoy/v2/debug.go getResourceVersion in Istio pilot before 1.5.0-alpha.0. If a particular HTTP GET request is made to the pilot API endpoint, it is possible to cause the Go runtime to panic (resulting in a denial of service to the istio-pilot application).	2021-01-29	not yet calculated	CVE-2019-25014 MISC MISC
jenkins -- jenkins	Jenkins 2.275 and LTS 2.263.2 allows reading arbitrary files using the file browser for workspaces and archived artifacts due to a time-of-check to time-of-use (TOCTOU) race condition.	2021-01-26	not yet calculated	CVE-2021-21615 MLIST CONFIRM
jp2_ decode -- jp2_decode	jp2_decode in jp2/jp2_dec.c in libjasper in JasPer 2.0.24 has a heap-based buffer over-read when there is an invalid relationship between the number of channels and the number of image components.	2021-01-27	not yet calculated	CVE-2021-3272 MISC
jxbrowser -- ti_code_composer_studio_ide	jxbrowser in TI Code Composer Studio IDE 8.x through 10.x before 10.1.1 does not verify X.509 certificates for HTTPS.	2021-01-26	not yet calculated	CVE-2021-3285 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
klog -- klog_server	KLog Server through 2.4.1 allows authenticated command injection. async.php calls shell_exec() on the original value of the source parameter.	2021-01-26	not yet calculated	CVE-2021-3317 MISC
late-static -- late-static	An issue was discovered in the late-static crate before 0.4.0 for Rust. Because Sync is implemented for LateStatic with T: Send, a data race can occur.	2021-01-26	not yet calculated	CVE-2020-36209 MISC
lazy-init -- lazy-init	An issue was discovered in the lazy-init crate through 2021-01-17 for Rust. Lazy lacks a Send bound, leading to a data race.	2021-01-26	not yet calculated	CVE-2021-25901 MISC
libgcrypt -- libgcrypt	_gcry_md_block_write in cipher/hash-common.c in Libgcrypt before 1.9.1 has a heap-based buffer overflow when the digest final function sets a large count value.	2021-01-29	not yet calculated	CVE-2021-3345 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	A flaw incorrect umask during file or directory modification in the Linux kernel NFS (network file system) functionality was found in the way user create and delete object using NFSv4.2 or newer if both simultaneously accessing the NFS by the other process that is not using new NFSv4.2. A user with access to the NFS could use this flaw to starve the resources causing denial of service.	2021-01-26	not yet calculated	CVE-2020-35513 MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.	2021-01-29	not yet calculated	CVE-2021-3347 MLIST MLIST MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
local_service -- search_engine_management	Local Service Search Engine Management System 1.0 has a vulnerability through authentication bypass using SQL injection . Using this vulnerability, an attacker can bypass the login page.	2021-01-26	not yet calculated	CVE-2021-3278 MISC MISC
logstorage -- logstorage	Logstorage version 8.0.0 and earlier, and ELC Analytics version 3.0.0 and earlier allow remote attackers to execute arbitrary OS commands via a specially crafted log file.	2021-01-28	not yet calculated	CVE-2020-5626 MISC MISC
m&m_software -- fdtcontainer_component	M&M Software fdtCONTAINER Component in versions below 3.5.20304.x and between 3.6 and 3.6.20304.x is vulnerable to deserialization of untrusted data in its project storage.	2021-01-22	not yet calculated	CVE-2020-12525 CONFIRM MISC
madcodehook -- madcodehook	A TOCTOU vulnerability exists in madCodeHook before 2020-07-16 that allows local attackers to elevate their privileges to SYSTEM. This occurs because path redirection can occur via vectors involving directory junctions.	2021-01-30	not yet calculated	CVE-2020-14418 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
marc_crate -- marc_crate	An issue was discovered in the marc crate before 2.0.0 for Rust. A user-provided Read implementation can gain access to the old contents of newly allocated memory, violating soundness.	2021-01-29	not yet calculated	CVE-2021-26308 MISC
matrikon -- opc_ua_tunneller	The affected product is vulnerable to a heap-based buffer overflow, which may allow an attacker to manipulate memory with controlled values and remotely execute code on the OPC UA Tunneller (versions prior to 6.3.0.8233).	2021-01-26	not yet calculated	CVE-2020-27297 MISC
matrikon -- opc_ua_tunneller	The affected product is vulnerable to an out-of-bounds read, which may allow an attacker to obtain and disclose sensitive data information or cause the device to crash on the OPC UA Tunneller (versions prior to 6.3.0.8233).	2021-01-26	not yet calculated	CVE-2020-27299 MISC
matrikon -- opc_ua_tunneller	The affected product has uncontrolled resource consumption issues, which may allow an attacker to cause a denial-of-service condition on the OPC UA Tunneller (versions prior to 6.3.0.8233).	2021-01-26	not yet calculated	CVE-2020-27295 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
matrikon -- opc_ua_tunneller	Some parsing functions in the affected product do not check the return value of malloc and the thread handling the message is forced to close, which may lead to a denial-of-service condition on the OPC UA Tunneller (versions prior to 6.3.0.8233).	2021-01-26	not yet calculated	CVE-2020-27274 MISC
mautic -- mautic	A cross-site scripting (XSS) vulnerability in the assets component of Mautic before 3.2.4 allows remote attackers to inject executable JavaScript through the Referer header of asset downloads.	2021-01-28	not yet calculated	CVE-2020-35124 MISC MISC MISC MISC
may_queue -- may_queue	An issue was discovered in the may_queue crate through 2020-11-10 for Rust. Because Queue does not have bounds on its Send trait or Sync trait, memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36217 MISC
mediawiki -- mediawiki	The API in the Push extension for MediaWiki through 1.35 did not require an edit token in ApiPushBase.php and therefore facilitated a CSRF attack.	2021-01-29	not yet calculated	CVE-2020-29004 MISC CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM MISC
mediawiki -- mediawiki	The API in the Push extension for MediaWiki through 1.35 used cleartext for ApiPush credentials, allowing for potential information disclosure.	2021-01-29	not yet calculated	CVE-2020-29005 MISC MISC
melfa -- fr_series_controllers	Resource management errors vulnerability in a robot controller of MELFA FR Series(controller "CR800-*V*D" of RV-*FR***-D-* all versions, controller "CR800-*HD" of RH-*FRH***-D-* all versions, controller "CR800-*HRD" of RH-*FRHR***-D-* all versions, controller "CR800-*V*R with R16RTCPU" of RV-*FR***-R-* all versions, controller "CR800-*HR with R16RTCPU" of RH-*FRH***-R-* all versions, controller "CR800-*HRR with R16RTCPU" of RH-*FRHR***-R-* all versions, controller "CR800-*V*Q with Q172DSRCPU" of RV-*FR***-Q-* all versions, controller "CR800-*HQ with Q172DSRCPU" of RH-*FRH***-Q-* all versions, controller "CR800-*HRQ with Q172DSRCPU" of RH-*FRHR***-Q-* all versions) and a robot controller of MELFA CR	2021-01-29	not yet calculated	CVE-2021-20586 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Series(controller "CR800-CVD" of RV-8CRL-D-* all versions, controller "CR800-CHD" of RH-*CRH**-D-* all versions) as well as a cooperative robot ASSISTA(controller "CR800-05VD" of RV-5AS-D-* all versions) allows a remote unauthenticated attacker to cause a DoS of the execution of the robot program and the Ethernet communication by sending a large amount of packets in burst over a short period of time. As a result of DoS, an error may occur. A reset is required to recover it if the error occurs.			
micrium -- uchttp	A denial-of-service vulnerability exists in the HTTP Server functionality of Micrium uC-HTTP 3.01.00. A specially crafted HTTP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	2021-01-26	not yet calculated	CVE-2020-13582 MISC
microsoft -- windows	Insider Threat Management Windows Agent Local Privilege Escalation Vulnerability The Proofpoint Insider Threat Management (formerly ObserveIT) Agent for Windows before 7.4.3, 7.5.4, 7.6.5, 7.7.5, 7.8.4, 7.9.3, 7.10.2, and 7.11.0.25 as well as versions 7.3 and earlier is missing authentication for a critical function, which allows a local authenticated	2021-01-26	not yet calculated	CVE-2021-22159 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Windows user to run arbitrary commands with the privileges of the Windows SYSTEM user. Agents for MacOS, Linux, and ITM Cloud are not affected.			
mitel -- businesscti_enterprise_client_for_windows	The chat window of the Mitel BusinessCTI Enterprise (MBC-E) Client for Windows before 6.4.15 and 7.x before 7.1.2 could allow an attacker to gain access to user information by sending certain code, due to improper input validation of http links. A successful exploit could allow an attacker to view user information and application data.	2021-01-29	not yet calculated	CVE-2021-3176 MISC CONFIRM
mitel -- micollab	A library index page in NuPoint Messenger in Mitel MiCollab before 9.2 FP1 could allow an unauthenticated attacker to gain access (view and modify) to user data.	2021-01-29	not yet calculated	CVE-2020-35547 MISC CONFIRM
monitorix -- monitorix	Monitorix 3.13.0 allows remote attackers to bypass Basic Authentication in a default installation (i.e., an installation without a hosts_deny option). This issue occurred because a new access-control feature was introduced without considering that some exiting	2021-01-27	not yet calculated	CVE-2021-3325 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	installations became unsafe, upon an update to 3.13.0, unless the new feature was immediately configured.			MISC CONFIRM
moodle -- moodle	It was found in Moodle before version 3.10.1, 3.9.4 and 3.8.7 that a insufficient capability checks in some grade related web services meant students were able to view other students grades.	2021-01-28	not yet calculated	CVE-2021-20184 MISC
moodle -- moodle	It was found in Moodle before version 3.10.1, 3.9.4, 3.8.7 and 3.5.16 that it was possible for site administrators to execute arbitrary PHP scripts via a PHP include used during Shibboleth authentication.	2021-01-28	not yet calculated	CVE-2021-20187 MISC
moodle -- moodle	It was found in Moodle before version 3.10.1 that some search inputs were vulnerable to reflected XSS due to insufficient escaping of search queries.	2021-01-28	not yet calculated	CVE-2021-20183 MISC
moodle -- moodle	It was found in Moodle before version 3.10.1, 3.9.4, 3.8.7 and 3.5.16 that messaging did not impose a character limit when sending messages, which could	2021-01-28	not yet calculated	CVE-2021-20185 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result in client-side (browser) denial of service for users receiving very large messages.			
moodle -- moodle	It was found in Moodle before version 3.10.1, 3.9.4, 3.8.7 and 3.5.16 that if the TeX notation filter was enabled, additional sanitizing of TeX content was required to prevent the risk of stored XSS.	2021-01-28	not yet calculated	CVE-2021-20186 MISC
multiqueue2 -- multiqueue2	An issue was discovered in the multiqueue2 crate before 0.1.7 for Rust. Because a non-Send type can be sent to a different thread, a data race can occur.	2021-01-26	not yet calculated	CVE-2020-36214 MISC
mybb -- mybb	The Hide-Thread-Content plugin through 2021-01-27 for MyBB allows remote attackers to bypass intended content-reading restrictions by clicking on reply or quote in the postbit.	2021-01-28	not yet calculated	CVE-2021-3337 MISC MISC
nagios -- docker_config_wizard	Improper access and command validation in the Nagios Docker Config Wizard before 1.1.2, as used in Nagios XI through 5.7, allows an unauthenticated attacker to execute remote code as the apache user.	2021-01-26	not yet calculated	CVE-2021-3193 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
newbee-mall -- newbee-mall	newbee-mall all versions are affected by incorrect access control to remotely gain privileges through NewBeeMallIndexConfigServiceImpl.java. Unauthorized changes can be made to any user information through the userID.	2021-01-26	not yet calculated	CVE-2020-23449 MISC
newbee-mall -- newbee-mall	newbee-mall all versions are affected by incorrect access control to remotely gain privileges through AdminLoginInterceptor.java. The authentication logic of the system's background /admin is in code AdminLoginInterceptor, which can be bypassed.	2021-01-26	not yet calculated	CVE-2020-23448 MISC
nextcloud -- nextcloud_server	A missing input validation in Nextcloud Server before 20.0.2, 19.0.5, 18.0.11 allows users to store unlimited data in workflow rules causing load and potential DDoS on later interactions and usage with those rules.	2021-01-26	not yet calculated	CVE-2020-8293 MISC MISC
nextcloud -- nextcloud_server	A wrong check in Nextcloud Server 19 and prior allowed to perform a denial of service attack when resetting the password for a user.	2021-01-26	not yet calculated	CVE-2020-8295 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nibbleblog -- nibbleblog	dmin/kernel/api/login.class.phpin in nibbleblog v3.7.1c allows type juggling for login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2021-01-27	not yet calculated	CVE-2020-23356 MISC
nim -- nim	In Nim before 1.2.6, the standard library asyncftpclient lacks a check for whether a message contains a newline character.	2021-01-30	not yet calculated	CVE-2020-15690 MISC CONFIRM
node-red-contrib-huemagic -- node-red-contrib-huemagic	node-red-contrib-huemagic 3.0.0 is affected by hue/assets/..%2F Directory Traversal.in the res.sendFile API, used in file hue-magic.js, to fetch an arbitrary file.	2021-01-26	not yet calculated	CVE-2021-25864 MISC
nutch -- dmozparser	An XML external entity (XXE) injection vulnerability was discovered in the Nutch DmozParser and is known to affect Nutch versions < 1.18. XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing	2021-01-25	not yet calculated	CVE-2021-23901 CONFIRM CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access. This issue is fixed in Apache Nutch 1.18.			RM MLIST MLIST
nvidia -- multiple_products	NVIDIA Tegra kernel in Jetson AGX Xavier Series, Jetson Xavier NX, TX1, TX2, Nano and Nano 2GB, all L4T versions prior to r32.5, contains a vulnerability in the INA3221 driver in which improper access control may lead to unauthorized users gaining access to system power usage data, which may lead to information disclosure.	2021-01-26	not yet calculated	CVE-2021-1071 CONFIRM
nvidia -- multiple_products	NVIDIA Jetson AGX Xavier Series, Jetson Xavier NX, TX1, TX2, Nano and Nano 2GB, L4T versions prior to 32.5, contains a vulnerability in the apply_binaries.sh script used to install NVIDIA components into the root file system image, in which improper access control is applied, which may lead to an unprivileged user being able to modify system device tree files, leading to denial of service.	2021-01-26	not yet calculated	CVE-2021-1070 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
octopusdsc -- octopusdsc	OctopusDSC is a PowerShell module with DSC resources that can be used to install and configure an Octopus Deploy Server and Tentacle agent. In OctopusDSC version 4.0.977 and earlier a customer API key used to connect to Octopus Server is exposed via logging in plaintext. This vulnerability is patched in version 4.0.1002.	2021-01-22	not yet calculated	CVE-2021-21270 MISC MISC MISC CONFIRM
oncommand -- unified_manager_core_package	OnCommand Unified Manager Core Package versions prior to 5.2.5 may disclose sensitive account information to unauthorized users via the use of PuTTY Link (plink).	2021-01-28	not yet calculated	CVE-2020-8585 MISC CONFIRM
online_news_portal -- online_news_portal	Online News Portal using PHP/MySQLi 1.0 is affected by cross-site scripting (XSS) which allows remote attackers to inject an arbitrary web script or HTML via the "Title" parameter.	2021-01-26	not yet calculated	CVE-2020-29241 MISC
onlyoffice -- document_server	Directory traversal with remote code execution can occur in /upload in ONLYOFFICE Document	2021-01-26	not yet calculated	CVE-2021-3199

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Server before 5.6.3, when JWT is used, via a /.. sequence in an image upload parameter.			MISC CONFIRM
open5gs -- open5gs	Open5GS 2.1.3 listens on 0.0.0.0:3000 and has a default password of 1423 for the admin account.	2021-01-26	not yet calculated	CVE-2021-25863 MISC
openemr -- openemr	A cross-site request forgery vulnerability exists in the GACL functionality of OpenEMR 5.0.2 and development version 6.0.0 (commit babec93f600ff1394f91ccd512bcad85832eb6ce). A specially crafted HTTP request can lead to the execution of arbitrary requests in the context of the victim. An attacker can send an HTTP request to trigger this vulnerability.	2021-01-28	not yet calculated	CVE-2020-13569 MISC
openjpeg2 -- openjpeg2	A heap-buffer overflow was found in the way openjpeg2 handled certain PNG format files. An attacker could use this flaw to cause an application crash or in some cases execute arbitrary code with the permission of the user running such an application.	2021-01-26	not yet calculated	CVE-2020-27814 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				GENTOO
openmaint -- openmaint	openMAINT before 1.1-2.4.2 allows remote authenticated users to run arbitrary JSP code on the underlying web server.	2021-01-26	not yet calculated	CVE-2020-24549 MISC MISC
opensolution -- quick	OpenSolution Quick.CMS < 6.7 and Quick.Cart < 6.7 allow an authenticated user to perform code injection (and consequently Remote Code Execution) via the input fields of the Language tab.	2021-01-28	not yet calculated	CVE-2020-35754 MISC MISC CONFIRM MISC
oras -- oras	ORAS is open source software which enables a way to push OCI Artifacts to OCI Conformant registries. ORAS is both a CLI for initial testing and a Go Module. In ORAS from version 0.4.0 and before version 0.9.0, there is a "zip-slip" vulnerability. The directory support feature allows the downloaded	2021-01-25	not yet calculated	CVE-2021-21272 MISC MISC CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	gzipped tarballs to be automatically extracted to the user-specified directory where the tarball can have symbolic links and hard links. A well-crafted tarball or tarballs allow malicious artifact providers linking, writing, or overwriting specific files on the host filesystem outside of the user-specified directory unexpectedly with the same permissions as the user who runs `oras pull`. Users of the affected versions are impacted if they are `oras` CLI users who runs `oras pull`, or if they are Go programs, which invoke `github.com/deislabs/oras/pkg/content.FileStore`. The problem has been fixed in version 0.9.0. For `oras` CLI users, there is no workarounds other than pulling from a trusted artifact provider. For `oras` package users, the workaround is to not use `github.com/deislabs/oras/pkg/content.FileStore`, and use other content stores instead, or pull from a trusted artifact provider.			RM MISC
oscommerce -- oscommerce	oscommerce v2.3.4.1 has a functional problem in user registration and password rechecking, where a non-identical password can bypass the checks in /catalog/admin/administrators.php and /catalog/password_reset.php	2021-01-27	not yet calculated	CVE-2020-23360 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
persis -- human_resouce_management_portal	The job posting recommendation form in Persis Human Resource Management Portal (Versions 17.2.00 through 17.2.35 and 19.0.00 through 19.0.20), when the "Recommend job posting" function is enabled, allows XSS via the SENDER parameter.	2021-01-26	not yet calculated	CVE-2020-35753 MISC
philips -- interventional_workspot	Philips Interventional Workspot (Release 1.3.2, 1.4.0, 1.4.1, 1.4.3, 1.4.5), Coronary Tools/Dynamic Coronary Roadmap/Stentboost Live (Release 1.0), ViewForum (Release 6.3V1L10). The software constructs all or part of an OS command using externally influenced input from an upstream component but does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when sent to a downstream component.	2021-01-26	not yet calculated	CVE-2020-27298 MISC
phplist -- phplist	phpList 3.6.0 allows CSV injection, related to the email parameter, and /lists/admin/ exports.	2021-01-26	not yet calculated	CVE-2021-3188 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phplist -- phplist	phpList 3.5.3 allows type juggling for login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2021-01-27	not yet calculated	CVE-2020-23361 MISC
projectsend -- projectsend	reset-password.php in ProjectSend before r1295 allows remote attackers to reset a password because of incorrect business logic. Errors are not properly considered (an invalid token parameter).	2021-01-26	not yet calculated	CVE-2020-28874 MISC CONFIRM MISC CONFIRM MISC
pyrescom -- termod4_time_management_devices	Local file inclusion in Pyrescom Termod4 time management devices before 10.04k allows authenticated remote attackers to traverse directories and read sensitive files via the Maintenance > Logs menu and manipulating the file-path in the URL.	2021-01-26	not yet calculated	CVE-2020-23161 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pyrescom -- termod4_time_management_devices	Sensitive information disclosure and weak encryption in Pyrescom Termod4 time management devices before 10.04k allows remote attackers to read a session-file and obtain plain-text user credentials.	2021-01-26	not yet calculated	CVE-2020-23162 MISC MISC
qdocs -- smart_hospital_management_system	A cross-site scripting (XSS) issue in Add Patient Form in QDOCS Smart Hospital Management System 3.1 allows a remote attacker to inject arbitrary code via the Name, Guardian Name, Email, Address, Remarks, or Any Known Allergies field.	2021-01-26	not yet calculated	CVE-2020-36011 MISC MISC
qemu -- qemu	A flaw was found in qemu. A host privilege escalation issue was found in the virtio-fs shared file system daemon where a privileged guest user is able to create a device special file in the shared directory and use it to r/w access host devices.	2021-01-28	not yet calculated	CVE-2020-35517 MISC MISC MISC MISC
qemu -- sdhci_devices	A heap-based buffer overflow was found in QEMU through 5.0.0 in the SDHCI device emulation support. It could occur while doing a multi block SDMA transfer via the	2021-01-30	not yet calculated	CVE-2020-17380 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sdhci_sdma_transfer_multi_blocks() routine in hw/sd/sdhci.c. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition, or potentially execute arbitrary code with privileges of the QEMU process on the host.			RM CONFIRM
raw-cpuid_crate -- raw-cpuid_crate	An issue was discovered in the raw-cpuid crate before 9.0.0 for Rust. It has unsound transmute calls within as_string() methods.	2021-01-29	not yet calculated	CVE-2021-26306 MISC
raw-cpuid_crate -- raw-cpuid_crate	An issue was discovered in the raw-cpuid crate before 9.0.0 for Rust. It allows __cpuid_count() calls even if the processor does not support the CPUID instruction, which is unsound and causes a deterministic crash.	2021-01-29	not yet calculated	CVE-2021-26307 MISC
redhat -- keycloak	A flaw was found in keycloak before version 13.0.0. In some scenarios a user still has access to a resource after changing the role mappings in Keycloak and after expiration of the previous access token.	2021-01-28	not yet calculated	CVE-2020-1725 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redhat -- keycloak	The logout endpoint /oauth/logout?redirect=url can be abused to redirect logged in users to arbitrary web pages. This vulnerability could be used in phishing attacks. Versions shipped with Red Hat Mobile Aplication Platform 4 are believed to be vulnerable.	2021-01-28	not yet calculated	CVE-2020-1723 MISC
reffers -- reffers	An issue was discovered in the reffers crate through 2020-12-01 for Rust. ARefss can contain a !Send,!Sync object, leading to a data race and memory corruption.	2021-01-26	not yet calculated	CVE-2020-36203 MISC
revive -- adserver	Revive Adserver before 5.1.0 permits any user with a manager account to store possibly malicious content in the URL website property, which is then displayed unsanitized in the affiliate-preview.php tag generation screen, leading to a persistent cross-site scripting (XSS) vulnerability.	2021-01-26	not yet calculated	CVE-2021-22871 MISC FULLDISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
revive -- adserver	Revive Adserver before 5.1.0 is vulnerable to a reflected cross-site scripting (XSS) vulnerability via the publicly accessible afr.php delivery script. While this issue was previously addressed in modern browsers as CVE-2020-8115, some older browsers (e.g., IE10) that do not automatically URL encode parameters were still vulnerable.	2021-01-26	not yet calculated	CVE-2021-22872 MISC FULLDISC MISC MISC MISC MISC
revive -- adserver	Revive Adserver before 5.1.0 is vulnerable to open redirects via the `dest`, `oadest`, and/or `ct0` parameters of the lg.php and ck.php delivery scripts. Such open redirects had previously been available by design to allow third party ad servers to track such metrics when delivering ads. However, third party click tracking via redirects is not a viable option anymore, leading to such open redirect functionality being removed and reclassified as a vulnerability.	2021-01-26	not yet calculated	CVE-2021-22873 MISC FULLDISC MISC MISC MISC
riolink -- p2p_products	The affected Reolink P2P products do not sufficiently protect data transferred between the local device and Reolink servers. This can allow an	2021-01-26	not yet calculated	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to access sensitive information, such as camera feeds.			25169 MISC
riolink -- p2p_products	An attacker with local network access can obtain a fixed cryptography key which may allow for further compromise of Reolink P2P cameras outside of local network access	2021-01-26	not yet calculated	CVE-2020-25173 MISC
rocket.chat -- rocket.chat	The `specializedRendering` function in Rocket.Chat server before 3.9.2 allows a cross-site scripting (XSS) vulnerability by way of the `value` parameter.	2021-01-26	not yet calculated	CVE-2020-8288 MISC MISC MISC
rostelecom -- cs-c2shw	Denial of Service vulnerability in Rostelecom CS-C2SHW 5.0.082.1. AgentGreen service has a bug in parsing broadcast discovery UDP packet. Sending a packet of too small size will lead to an attempt of allocating buffer of negative size. As the result service AgentGreen will be terminated and started again later.	2021-01-26	not yet calculated	CVE-2020-27541 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rostelecom -- cs-c2shw	Rostelecom CS-C2SHW 5.0.082.1 is affected by: Bash command injection. The camera reads configuration from QR code (including network settings). The static IP configuration from QR code is copied to the file /config/ip-static and after reboot data from this file is inserted into bash command (without any escaping). So bash injection is possible. Camera doesn't parse QR codes if it's already successfully configured. Camera is always rebooted after successful configuration via QR code.	2021-01-26	not yet calculated	CVE-2020-27542 MISC
rostelecom -- cs-c2shw	Bash injection vulnerability and bypass of signature verification in Rostelecom CS-C2SHW 5.0.082.1. The camera reads firmware update configuration from SD card file vc\version.json. fw-sign parameter and from this configuration is directly inserted into a bash command. Firmware update is run automatically if there is special file on the inserted SD card.	2021-01-26	not yet calculated	CVE-2020-27540 MISC
rostelecom -- cs-c2shw	Heap overflow with full parsing of HTTP respose in Rostelecom CS-C2SHW 5.0.082.1. AgentUpdater service has a self-written HTTP parser and builder. HTTP parser has a heap buffer overflow (OOB write). In default configuration camera parses	2021-01-26	not yet calculated	CVE-2020-27539 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	responses only from HTTPS URLs from config file, so vulnerable code is unreachable and one more bug required to reach it.			
rsshub -- rsshub	RSSHub is an open source, easy to use, and extensible RSS feed generator. In RSSHub before version 7f1c430 (non-semantic versioning) there is a risk of code injection. Some routes use `eval` or `Function constructor`, which may be injected by the target site with unsafe code, causing server-side security issues The fix in version 7f1c430 is to temporarily remove the problematic route and added a `no-new-func` rule to eslint.	2021-01-26	not yet calculated	CVE-2021-21278 MISC CONFIRM MISC
rusb -- rusb	An issue was discovered in the rusb crate before 0.7.0 for Rust. Because of a lack of Send and Sync bounds, a data race and memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36206 MISC
sagemcom -- f@st_3686_v2_3.495_devices	Sagemcom F@ST 3686 v2 3.495 devices have a buffer overflow via a long sessionKey to the goform/login URI.	2021-01-26	not yet calculated	CVE-2021-3304 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sangoma -- asterisk	An issue was discovered in res_pjsip_diversion.c in Sangoma Asterisk before 13.38.0, 14.x through 16.x before 16.15.0, 17.x before 17.9.0, and 18.x before 18.1.0. A crash can occur when a SIP message is received with a History-Info header that contains a tel-uri, or when a SIP 181 response is received that contains a tel-uri in the Diversion header.	2021-01-29	not yet calculated	CVE-2020-35652 CONFIRM CONFIRM MISC MISC
smallvec -- smallvec	An issue was discovered in the smallvec crate before 0.6.14 and 1.x before 1.6.1 for Rust. There is a heap-based buffer overflow in SmallVec::insert_many.	2021-01-26	not yet calculated	CVE-2021-25900 MISC
smartagent -- smartagent	SmartAgent 3.1.0 allows a ViewOnly attacker to create a SuperUser account via the /#/CampaignManager/users URI.	2021-01-26	not yet calculated	CVE-2021-3165 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
spring_cloud -- data_flow	In Spring Cloud Data Flow, versions 2.6.x prior to 2.6.5, versions 2.5.x prior 2.5.4, an application is vulnerable to SQL injection when requesting task execution.	2021-01-27	not yet calculated	CVE-2020-5427 CONFIRM
spring_cloud -- task	In applications using Spring Cloud Task 2.2.4.RELEASE and below, may be vulnerable to SQL injection when exercising certain lookup queries in the TaskExplorer.	2021-01-27	not yet calculated	CVE-2020-5428 CONFIRM
student_result_management_system -- student_result_management_system	Student Result Management System In PHP With Source Code is affected by SQL injection. An attacker can able to access of Admin Panel and manage every account of Result.	2021-01-26	not yet calculated	CVE-2020-35270 MISC MISC
sudo -- sudo	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.	2021-01-26	not yet calculated	CVE-2021-3156 MISC MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST FEDORA FEDORA GENTOO CONFIRM CONFIRM CISCO DEBIAN MISC CONFIRM
tenda -- ac5_ac1200	A Stored Cross-site scripting (XSS) vulnerability in /main.html Wifi Settings in Tenda AC5 AC1200 version V15.03.06.47_multi allows remote attackers to inject arbitrary web script or HTML via the Wifi Name parameter.	2021-01-26	not yet calculated	CVE-2021-3186 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tendermint -- tendermint_core	Tendermint Core is an open source Byzantine Fault Tolerant (BFT) middleware that takes a state transition machine - written in any programming language - and securely replicates it on many machines. Tendermint Core v0.34.0 introduced a new way of handling evidence of misbehavior. As part of this, we added a new Timestamp field to Evidence structs. This timestamp would be calculated using the same algorithm that is used when a block is created and proposed. (This algorithm relies on the timestamp of the last commit from this specific block.) In Tendermint Core v0.34.0-v0.34.2, the consensus reactor is responsible for forming DuplicateVoteEvidence whenever double signs are observed. However, the current block is still “in flight” when it is being formed by the consensus reactor. It hasn’t been finalized through network consensus yet. This means that different nodes in the network may observe different “last commits” when assigning a timestamp to DuplicateVoteEvidence. In turn, different nodes could form DuplicateVoteEvidence objects at the same height but with different timestamps. One DuplicateVoteEvidence object (with one timestamp) will then eventually get finalized in the block, but this means that any DuplicateVoteEvidence with a	2021-01-26	not yet calculated	CVE-2021-21271 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	different timestamp is considered invalid. Any node that formed invalid DuplicateVoteEvidence will continue to propose invalid evidence; its peers may see this, and choose to disconnect from this node. This bug means that double signs are DoS vectors in Tendermint Core v0.34.0-v0.34.2. Tendermint Core v0.34.3 is a security release which fixes this bug. As of v0.34.3, DuplicateVoteEvidence is no longer formed by the consensus reactor; rather, the consensus reactor passes the Votes themselves into the EvidencePool, which is now responsible for forming DuplicateVoteEvidence. The EvidencePool has timestamp info that should be consistent across the network, which means that DuplicateVoteEvidence formed in this reactor should have consistent timestamps. This release changes the API between the consensus and evidence reactors.			
terramaster -- terramaster_tos	TerraMaster TOS before 4.1.29 has Invalid Parameter Checking that leads to code injection as root. This is a dynamic class method invocation vulnerability in include/exportUser.php, in which an attacker can trigger a call to the exec method with (for example) OS commands in the opt parameter.	2021-01-30	not yet calculated	CVE-2020-15568 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
textpattern -- textpattern	Textpattern 4.8.4 is affected by cross-site scripting (XSS) in the Body parameter.	2021-01-26	not yet calculated	CVE-2020-35854 MISC MISC MISC
tibco -- bpm_enterprise_and_bpm_enterprise_distribution	The Application Development Clients component of TIBCO Software Inc.'s TIBCO BPM Enterprise and TIBCO BPM Enterprise Distribution for TIBCO Silver Fabric contains a vulnerability that theoretically allows a low privileged attacker with network access to execute a Cross Site Scripting (XSS) attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO BPM Enterprise: versions 4.3.0 and below and TIBCO BPM Enterprise Distribution for TIBCO Silver Fabric: versions 4.3.0 and below.	2021-01-26	not yet calculated	CVE-2021-23272 CONFIRM
tinycheck -- tinycheck	TinyCheck before commits 9fd360d and ea53de8 allowed an authenticated attacker to send an HTTP GET request to the crafted URLs.	2021-01-26	not yet calculated	CVE-2020-36200 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tinycheck -- tinycheck	TinyCheck before commits 9fd360d and ea53de8 was vulnerable to command injection due to insufficient checks of input parameters in several places.	2021-01-26	not yet calculated	CVE-2020-36199 MISC
tm_mobile_solutions -- testes_de_codigo	Mobile application "Testes de Codigo" v11.3 and prior allows stored XSS by injecting a payload in the "feedback" message field causing it to be stored in the remote database and leading to its execution on client devices when loading the "feedback list", either by accessing the website directly or using the mobile application.	2021-01-28	not yet calculated	CVE-2021-25647 MISC
tp-link -- tl-wr841N_v13	A Command Injection issue in the traceroute feature on TP-Link TL-WR841N V13 (JP) with firmware versions prior to 201216 allows authenticated users to execute arbitrary code as root via shell metacharacters, a different vulnerability than CVE-2018-12577.	2021-01-26	not yet calculated	CVE-2020-35576 MISC MISC
trendmicro -- serverprotect	A memory exhaustion vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow a local attacker to craft specific files that can cause a denial-of-service on the affected product. The specific flaw	2021-01-27	not yet calculated	CVE-2021-25225

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exists within a scheduled scan component. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			N/A N/A
trendmicro -- serverprotect	A memory exhaustion vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow a local attacker to craft specific files that can cause a denial-of-service on the affected product. The specific flaw exists within a manual scan component. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-01-27	not yet calculated	CVE-2021-25224 N/A N/A
trendmicro -- serverprotect	A memory exhaustion vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow a local attacker to craft specific files that can cause a denial-of-service on the affected product. The specific flaw exists within a scan engine component. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-01-27	not yet calculated	CVE-2021-25226 N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendmirco -- housecall_for_home_networks	A DLL hijacking vulnerability Trend Micro HouseCall for Home Networks version 5.3.1063 and below could allow an attacker to use a malicious DLL to escalate privileges and perform arbitrary code execution. An attacker must already have user privileges on the machine to exploit this vulnerability.	2021-01-27	not yet calculated	CVE-2021-25247 N/A
va-ts -- va-ts	An issue was discovered in the va-ts crate before 0.0.4 for Rust. Because Demuxer<T> omits a required T: Send bound, a data race and memory corruption can occur.	2021-01-26	not yet calculated	CVE-2020-36220 MISC
vis-timeline -- vis-timeline	This affects the package vis-timeline before 7.4.4. An attacker with the ability to control the items of a Timeline element can inject additional script code into the generated application.	2021-01-22	not yet calculated	CVE-2020-28487 CONFIRM CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
webid -- webid	WeBid 1.2.2 admin/newuser.php has an issue with password rechecking during registration because it uses a loose comparison to check the identicalness of two passwords. Two non-identical passwords can still bypass the check.	2021-01-27	not yet calculated	CVE-2020-23359 MISC
wekan -- wekan	packages/wekan-ldap/server/ldap.js in Wekan before 4.87 can process connections even though they are not authorized by the Certification Authority trust store,	2021-01-26	not yet calculated	CVE-2021-3309 MISC MISC MISC
wing_ftp -- wing_ftp	An XSS issue was discovered in Wing FTP 6.4.4. An arbitrary IFRAME element can be included in the help pages via a crafted link, leading to the execution of (sandboxed) arbitrary HTML and JavaScript in the user's browser.	2021-01-26	not yet calculated	CVE-2020-27735 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
winmail -- winmail	A SSRF vulnerability exists in Winmail 6.5 in app.php in the key parameter when HTTPS is on. An attacker can use this vulnerability to cause the server to send a request to a specific URL. An attacker can modify the request header 'HOST' value to cause the server to send the request.	2021-01-26	not yet calculated	CVE-2020-23776 MISC
winmail -- winmail	A reflected XSS vulnerability exists in tohtml/convert.php of Winmail 6.5, which can cause JavaScript code to be executed.	2021-01-26	not yet calculated	CVE-2020-23774 MISC
winscp -- winscp	WinSCP before 5.17.10 allows remote attackers to execute arbitrary programs when the URL handler encounters a crafted URL that loads session settings. (For example, this is exploitable in a default installation in which WinSCP is the handler for sftp:// URLs.)	2021-01-27	not yet calculated	CVE-2021-3331 MISC MISC MISC MISC
wolfssl -- tls13.c	DoTls13CertificateVerify in tls13.c in wolfSSL through 4.6.0 does not cease processing for certain anomalous peer behavior (sending an ED22519,	2021-01-29	not yet calculated	CVE-2021-3336 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ED448, ECC, or RSA signature without the corresponding certificate).			
xcb -- xcb	An issue was discovered in the xcb crate through 2020-12-10 for Rust. base::Error does not have soundness. Because of the public ptr field, a use-after-free or double-free can occur.	2021-01-26	not yet calculated	CVE-2020-36205 MISC
xen -- xen	An issue was discovered in Xen 4.12.3 through 4.12.4 and 4.13.1 through 4.14.x. An x86 HVM guest with PCI pass through devices can force the allocation of all IDT vectors on the system by rebooting itself with MSI or MSI-X capabilities enabled and entries setup. Such reboots will leak any vectors used by the MSI(-X) entries that the guest might had enabled, and hence will lead to vector exhaustion on the system, not allowing further PCI pass through devices to work properly. HVM guests with PCI pass through devices can mount a Denial of Service (DoS) attack affecting the pass through of PCI devices to other guests or the hardware domain. In the latter case, this would affect the entire host.	2021-01-26	not yet calculated	CVE-2021-3308 MLIST MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xerox -- workcentre_products	An issue was discovered in certain Xerox WorkCentre products. They do not properly encrypt passwords. This affects 3655, 3655i, 58XX, 58XXi 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi 78XX, 78XXi, 7970, 7970i, EC7836, and EC7856 devices.	2021-01-26	not yet calculated	CVE-2020-36201 MISC
yale -- wipc-303w_cameras	** DISPUTED ** The Yale WIPC-303W 2.21 through 2.31 camera is vulnerable to remote command execution (RCE) through command injection via the HTTP API. NOTE: This may be a duplicate of CVE-2020-10176 .	2021-01-26	not yet calculated	CVE-2020-23826 MISC
z-blogphp -- valyria	Z-BlogPHP 1.6.0 Valyria is affected by incorrect access control. PHP loose comparison and a magic hash can be used to bypass authentication. zb_user/plugin/passwordvisit/include.php:password visit_input_password() uses loose comparison to authenticate, which can be bypassed via magic hash values.	2021-01-27	not yet calculated	CVE-2020-23352 MISC
zen -- cart	Zen Cart 1.5.7b allows admins to execute arbitrary OS commands by inspecting an HTML radio input element (within the modules edit page) and inserting a command.	2021-01-26	not yet calculated	CVE-2021-3291 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ziv_automation -- 4cct-ea6-334126bf	Improper Authentication vulnerability in the cookie parameter of ZIV AUTOMATION 4CCT-EA6-334126BF allows a local attacker to perform modifications in several parameters of the affected device as an authenticated user.	2021-01-29	not yet calculated	CVE-2021-25910 CONFIRM
ziv_automation -- 4cct-ea6-334126bf	ZIV Automation 4CCT-EA6-334126BF firmware version 3.23.80.27.36371, allows an unauthenticated, remote attacker to cause a denial of service condition on the device. An attacker could exploit this vulnerability by sending specific packets to the port 7919.	2021-01-29	not yet calculated	CVE-2021-25909 CONFIRM
zte -- multiple_products	Some ZTE products have a DoS vulnerability. Due to the improper handling of memory release in some specific scenarios, a remote attacker can trigger the vulnerability by performing a series of operations, resulting in memory leak, which may eventually lead to device denial of service. This affects: ZXR10 9904, ZXR10 9908, ZXR10 9916, ZXR10 9904-S, ZXR10 9908-S; all versions up to V1.01.10.B12.	2021-01-26	not yet calculated	CVE-2021-21723 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zyxel -- nbg2105	On Zyxel NBG2105 V1.00(AAGU.2)C0 devices, setting the login cookie to 1 provides administrator access.	2021-01-26	not yet calculated	CVE-2021-3297 MISC MISC MISC