BULLETIN (SB21-032)

VULNERABILITY SUMMARY FOR THE WEEK OF

25TH JANUARY, 2021

Bulletin (SB21-032)
Vulnerability Summary for the Week of January 25, 2021

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by 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 Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis . The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available

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 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 in spx_restservice startflash_func function.	2021-01-29	7.2	CVE-2021-25137 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 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
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 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.	2021-01-29	7.2	CVE-2021-25132 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 setfwimagelocation_func function.	2021-01-29	7.2	CVE-2021-25131 MISC

HIGH Vulnerabilities

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 setactdir_func function.	2021-01-29	7.2	CVE-2021-25130 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 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 in spx_restservice generatesslcertificate_func function.	2021-01-29	7.2	CVE-2021-25127 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 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
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 root access due to improper access control. IBM X-Force ID: 192028.	2021-01-27	9	CVE-2020-4952 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 used. NOTE: this issue exists because of an incomplete fix for CVE-2020-35545.	2021-01-26	7.5	CVE-2021-3286 MISC

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 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.	2021-01-26	5	CVE-2020-17522 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
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
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
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-Simulator and V-Server Lite (versions prior to 4.0.10.0).	2021-01-27	6.8	CVE-2021-22639 MISC MISC
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
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

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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 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.	2021-01-27	4.3	CVE-2020-4816 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
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
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 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.	2021-01-29	6.5	CVE-2020-28405 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
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 bug_arr[]= in a crafted bug_actiongroup_page.php URL. (The target Issues can have Private view status, or belong to a private Project.)	2021-01-29	4	CVE-2020-29605 MISC MISC
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	2021-01-29	4	CVE-2020-29604 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Project) via the bug_arr[] parameter. This provides full access to potentially confidential information.			
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 project_id parameter, without having access to them.	2021-01-29	4	CVE-2020-29603 MISC MISC
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 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 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
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 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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
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
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 has been found that Item description is reflected without sanitization in app/items_view.php which enables the malicious scenario.	2021-01-22	3.5	CVE-2021-21260 MISC CONFIRM
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
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
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

Low Vulnerabilities

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