BULLETIN (SB20-062)

VULNERABILITY SUMMARY FOR THE WEEK OF 24 FEBRUARY, 20

Bulletin (SB20-062)
Vulnerability Summary for the Week of 24 February, 20

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
apache -- jsery_protocol	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.	2020-02-24	7.5	CVE-2020-1938 MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST CONFIRM
cacti -- cacti	graph_realtime.php in Cacti 1.2.8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in a cookie, if a guest user has the graph real-time privilege.	2020-02-22	9.3	CVE-2020-8813 MISC MISC MISC MISC CONFIRM MISC MISC
cisco -- fxos_software	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.	2020-02-26	7.2	CVE-2020-3169 CISCO
compile-sass -- compile-sass	compile-sass prior to 1.0.5 allows execution of arbritary commands. The function "setupCleanupOnExit(cssPath)" within "dist/index.js" is executed as part of the "rm" command without any sanitization.	2020-02-24	7.5	CVE-2019-10799 MISC MISC
couchbase -- couchbase_server	Couchbase Server 4.x and 5.x before 6.0.0 has Insecure Permissions for the projector and indexer REST endpoints (they allow unauthenticated access).	2020-02-22	7.5	CVE-2020-9039 CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dap-1330_devices	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-1330 1.10B01 BETA Wi-Fi range extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of cookies. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9554.	2020-02-22	8.3	CVE-2020-8861 N/A N/A
d-link -- dap-2610_devices	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-2610 Firmware v2.01RC067 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. The issue results from the lack of proper password checking. An attacker can leverage this vulnerability to execute arbitrary code in the context of root. Was ZDI-CAN-10082.	2020-02-22	8.3	CVE-2020-8862 N/A N/A
d-link -- dch-m225_devices	D-Link DCH-M225 1.05b01 and earlier devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the spotifyConnect.php userName parameter.	2020-02-21	10	CVE-2020-6841 MISC CONFIRM
d-link -- dch-m225_devices	D-Link DCH-M225 1.05b01 and earlier devices allow remote authenticated admins to execute arbitrary OS commands via shell metacharacters in the media renderer name.	2020-02-21	9	CVE-2020-6842 MISC CONFIRM
druva -- insync_macos_client	Improper neutralization of directives in dynamically evaluated code in Druva inSync Mac OS Client 6.5.0 allows a local, authenticated attacker to execute arbitrary Python expressions with root privileges.	2020-02-25	7.2	CVE-2019-4000 MISC
druva -- insync_windows_client	Improper neutralization of special elements used in an OS command in Druva inSync Windows Client 6.5.0 allows a local, unauthenticated attacker to execute arbitrary operating system commands with SYSTEM privileges.	2020-02-25	7.2	CVE-2019-3999 MISC
gnu -- screen	A buffer overflow was found in the way GNU Screen before 4.8.0 treated the special escape OSC 49. Specially crafted output, or a special program, could corrupt memory and crash Screen or possibly have unspecified other impact.	2020-02-24	7.5	CVE-2020-9366 MLIST MISC MISC
ibl_software_engineering -- online_weather	IBL Online Weather before 4.3.5a allows unauthenticated eval injection via the queryBCP method of the Auxiliary Service.	2020-02-26	7.5	CVE-2020-9406 MISC
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.	2020-02-24	10	CVE-2020-4212 XF CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175022.	2020-02-24	10	CVE-2020-4211 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175091.	2020-02-24	10	CVE-2020-4222 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175020.	2020-02-24	10	CVE-2020-4210 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175024.	2020-02-24	10	CVE-2020-4213 XF CONFIRM
moxa -- awk-3131a_devices	An exploitable command injection vulnerability exists in encrypted diagnostic script functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted diagnostic script file can cause arbitrary busybox commands to be executed, resulting in remote control over the device. An attacker can send diagnostic while authenticated as a low privilege user to trigger this vulnerability.	2020-02-25	9	CVE-2019-5138 MISC
moxa -- awk-3131a_devices	An exploitable privilege escalation vulnerability exists in the iw_console functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted menu selection string can cause an escape from the restricted console, resulting in system access as the root user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2020-02-25	9	CVE-2019-5136 MISC
moxa -- awk-3131a_devices	An exploitable command injection vulnerability exists in the hostname functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted entry to network configuration information can cause execution of arbitrary system commands, resulting in full control of the device. An attacker can send various authenticated requests to trigger this vulnerability.	2020-02-25	9	CVE-2019-5142 MISC
moxa -- awk-3131a_devices	An exploitable improper access control vulnerability exists in the iw_webs account settings functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted user name entry can cause the overwrite of an existing user account password, resulting in remote shell access to the device as that user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2020-02-25	9	CVE-2019-5162 MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netapp -- oncommand_cloud_manager	OnCommand Cloud Manager versions prior to 3.8.0 are susceptible to arbitrary code execution by remote attackers.	2020-02-26	7.5	CVE-2019-17275 CONFIRM
netgear -- nighthawk_x10-r900_devices	In NETGEAR Nighthawk X10-R900 prior to 1.0.4.26, an attacker may execute arbitrary system commands as root by sending a specially-crafted MAC address to the "NETGEAR Genie" SOAP endpoint at AdvancedQoS:GetCurrentBandwidthByMAC. Although this requires QoS being enabled, advanced QoS being enabled, and a valid authentication JWT, additional vulnerabilities (CVE-2019-12510) allow an attacker to interact with the entire SOAP API without authentication. Additionally, DNS rebinding techniques may be used to exploit this vulnerability remotely. Exploiting this vulnerability is somewhat involved. The following limitations apply to the payload and must be overcome for successful exploitation: - No more than 17 characters may be used. - At least one colon must be included to prevent mangling. - A single-quote and meta-character must be used to break out of the existing command. - Parent command remnants after the injection point must be dealt with. - The payload must be in all-caps. Despite these limitations, it is still possible to gain access to an interactive root shell via this vulnerability. Since the web server assigns certain HTTP headers to environment variables with all-caps names, it is possible to insert a payload into one such header and reference the subsequent environment variable in the injection point.	2020-02-24	9.3	CVE-2019-12511 MISC
networkmanager-ssh -- networkmanager-ssh	danfruehauf NetworkManager-ssh before 1.2.11 allows privilege escalation because extra options are mishandled.	2020-02-23	7.5	CVE-2020-9355 MISC MISC MISC
opensmtpd -- opensmtpd	OpenSMTPD before 6.6.4 allows remote code execution because of an out-of-bounds read in mta_io in mta_session.c for multi-line replies. Although this vulnerability affects the client side of OpenSMTPD, it is possible to attack a server because the server code launches the client code during bounce handling.	2020-02-25	10	CVE-2020-8794 FULLDISC MLIST MLIST MLIST DEBIAN MISC MISC
patriot -- viper_rgb	A buffer overflow was found in Patriot Viper RGB through 1.1 when processing IoControlCode 0x80102040. Local attackers (including low integrity processes) can exploit this to gain NT AUTHORITY\SYSTEM privileges.	2020-02-21	7.2	CVE-2019-19452 MISC MISC
ruby -- rake	There is an OS command injection vulnerability in Ruby Rake < 12.3.3 in Rake::FileList when supplying a filename that begins with the pipe character `|`.	2020-02-24	9.3	CVE-2020-8130 MISC MLIST
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. It allows blind Command Injection. An attacker without authentication is able to execute arbitrary operating system command by injecting the vulnerable parameter in the PHP Web page /common/vam_monitor_sap.php.	2020-02-26	10	CVE-2019-19994 MISC MISC MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
smartclient -- smartclient	An issue was discovered in SmartClient 12.0. Unauthenticated exploitation of blind XXE can occur in the downloadWSDL feature by sending a POST request to /tools/developerConsoleOperations.jsp with a valid payload in the _transaction parameter.	2020-02-23	7.5	CVE-2020-9352 MISC
tp-link -- tl-wr849n_devices	On TP-Link TL-WR849N 0.9.1 4.16 devices, a remote command execution vulnerability in the diagnostics area can be exploited when an attacker sends specific shell metacharacters to the panel's traceroute feature.	2020-02-24	7.5	CVE-2020-9374 MISC MISC
yarn -- yarn	Arbitrary filesystem write vulnerability in Yarn before 1.22.0 allows attackers to write to any path on the filesystem and potentially lead to arbitrary code execution by forcing the user to install a malicious package.	2020-02-24	7.5	CVE-2020-8131 CONFIRM MISC
zsh -- zsh	In Zsh before 5.8, attackers able to execute commands can regain privileges dropped by the --no-PRIVILEGED option. Zsh fails to overwrite the saved uid, so the original privileges can be restored by executing MODULE_PATH=/dir/with/module zmodload with a module that calls setuid().	2020-02-24	7.2	CVE-2019-20044 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- kylin	Kylin has some restful apis which will concatenate SQLs with the user input string, a user is likely to be able to run malicious database queries.	2020-02-24	4	CVE-2020-1937 MLIST
apache -- struts	Apache Struts before 2.3.20 has a cross-site scripting (XSS) vulnerability.	2020-02-27	4.3	CVE-2015-2992 MISC MISC MISC
atos -- unify_openscape_uc_application	Atos Unify OpenScape UC Application V9 before version V9 R4.31.0 and V10 before version V10 R0.6.0 allows XSS. An attacker could exploit this by convincing an authenticated user to inject arbitrary JavaScript code in the Profile Name field. A browser would execute this stored XSS payload.	2020-02-21	4.3	CVE-2019-19865 MISC MISC
atos -- unify_openscape_uc_web_client	Atos Unify OpenScape UC Web Client V9 before version V9 R4.31.0 and V10 before version V10 R0.6.0 allows remote attackers to obtain sensitive information. By iterating the value of conferenceId to getMailFunction in the JSON API, one can enumerate all conferences scheduled on the platform, with their numbers and access PINs.	2020-02-21	5	CVE-2019-19866 MISC MISC
auieo -- candid_applicant_tracking_system	CandidATS 2.1.0 is vulnerable to CSRF that allows for an administrator account to be added via the index.php?m=settings&a=addUser URI.	2020-02-22	6.8	CVE-2020-9341 MISC
buddypress -- buddypress	In BuddyPress before 5.1.2, requests to a certain REST API endpoint can result in private user data getting exposed. Authentication is not needed. This has been patched in version 5.1.2.	2020-02-24	5	CVE-2020-5244 MISC MISC CONFIRM
centreon -- centreon_web	An issue was discovered in Centreon Web through 19.04.3. When a user changes his password on his profile page, the contact_autologin_key field in the database becomes blank when it should be NULL. This makes it possible to partially bypass authentication.	2020-02-24	6.5	CVE-2019-15299 MISC MISC MISC
dnn_software -- dnn	DNN (formerly DotNetNuke) through 9.4.4 has Insecure Permissions.	2020-02-24	4	CVE-2020-5188 MISC MISC MISC
dnn_software -- dnn	DNN (formerly DotNetNuke) through 9.4.4 allows Path Traversal (issue 2 of 2).	2020-02-24	6.5	CVE-2020-5187 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
election -- election	fauzantrif eLection 2.0 has SQL Injection via the admin/ajax/op_kandidat.php id parameter.	2020-02-22	6.5	CVE-2020-9340 MISC
fiserv -- accurate_reconciliation	Fiserv Accurate Reconciliation 2.19.0 allows XSS via the logout.jsp timeOut parameter.	2020-02-26	4.3	CVE-2020-8952 MISC
freeradius -- pam_radius	add_password in pam_radius_auth.c in pam_radius 1.4.0 does not correctly check the length of the input password, and is vulnerable to a stack-based buffer overflow during memcpy(). An attacker could send a crafted password to an application (loading the pam_radius library) and crash it. Arbitrary code execution might be possible, depending on the application, C library, compiler, and other factors.	2020-02-24	5	CVE-2015-9542 CONFIRM MISC MLIST
gogs -- gogs	Gogs through 0.11.91 allows attackers to violate the admin-specified repo-creation policy due to an internal/db/repo.go race condition.	2020-02-21	4.3	CVE-2020-9329 MISC
golfbuddy -- course_manager	In GolfBuddy Course Manager 1.1, passwords are sent (with base64 encoding) via a GET request.	2020-02-26	4	CVE-2020-9337 MISC MISC
google -- android	btif/src/btif_dm.c in Android before 5.1 does not properly enforce the temporary nature of a Bluetooth pairing, which allows user-assisted remote attackers to bypass intended access restrictions via crafted Bluetooth packets after the tapping of a crafted NFC tag.	2020-02-21	5.8	CVE-2014-7914 MISC
google -- chrome	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-27	6.8	CVE-2020-6407 MISC MISC
google -- chrome	Use after free in speech in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-27	6.8	CVE-2020-6386 MISC MISC
google -- chrome	Use after free in WebAudio in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-27	6.8	CVE-2020-6384 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-27	4.3	CVE-2020-6418 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Type confusion in V8 in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-27	6.8	CVE-2020-6383 MISC MISC
gurux -- gxdlms_director	Gurux GXDLMS Director prior to 8.5.1905.1301 downloads updates to add-ins and OBIS code over an unencrypted HTTP connection. A man-in-the-middle attacker can prompt the user to download updates by modifying the contents of gurux.fi/obis/files.xml and gurux.fi/updates/updates.xml. Then, the attacker can modify the contents of downloaded files. In the case of add-ins (if the user is using those), this will lead to code execution. In case of OBIS codes (which the user is always using as they are needed to communicate with the energy meters), this can lead to code execution when combined with CVE-2020-8810.	2020-02-25	6.8	CVE-2020-8809 MISC MISC
ibl_software_engineering -- online_weather	IBL Online Weather before 4.3.5a allows attackers to obtain sensitive information by reading the IWEBSERVICE_JSONRPC_COOKIE cookie.	2020-02-26	5	CVE-2020-9407 MISC
ibl_software_engineering -- online_weather	IBL Online Weather before 4.3.5a allows unauthenticated reflected XSS via the redirect page.	2020-02-26	4.3	CVE-2020-9405 MISC
ibm -- business_process_manager_and_business_automation_workflow	IBM Business Process Manager 8.5.7.0 through 8.5.7.0 2017.06, 8.6.0.0 through 8.6.0.0 CF2018.03, and IBM Business Automation Workflow 18.0.0.1 through 19.0.0.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 171254.	2020-02-27	6.5	CVE-2019-4669 XF CONFIRM
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.1.0 could allow a remote attacker to disclose sensitive information to an authenticated user due to disclosing path information in the URL. IBM X-Force ID: 172883.	2020-02-24	4	CVE-2019-4745 XF CONFIRM
ibm -- qrader_advisor	IBM Qradar Advisor 1.1 through 2.5 with Watson uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 166206.	2020-02-25	5	CVE-2019-4557 XF CONFIRM
ibm -- qrader_advisor	IBM QRadar Advisor 1.1 through 2.5 could allow an unauthorized attacker to obtain sensitive information from specially crafted HTTP requests that could aid in further attacks against the system. IBM X-Force ID: 171438.	2020-02-25	5	CVE-2019-4672 XF CONFIRM
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability	2020-02-24	5.8	CVE-2019-4595 XF CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 167878.			
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 172363.	2020-02-26	4.3	CVE-2019-4726 XF CONFIRM
ibm -- sterling_brb_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 167881.	2020-02-26	6.5	CVE-2019-4598 XF CONFIRM
ibm -- sterling_brb_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 167880.	2020-02-26	6.5	CVE-2019-4597 XF CONFIRM
ibm -- websphere_service_registry_and_repository	IBM WebSphere Service Registry and Repository 8.5 could allow a user to obtain sensitive version information that could be used in further attacks against the system. IBM X-Force ID: 165593.	2020-02-26	5	CVE-2019-4537 XF CONFIRM
jetbrains -- scala_plugin	In the JetBrains Scala plugin before 2019.2.1, some artefact dependencies were resolved over unencrypted connections.	2020-02-21	5	CVE-2020-7907 MISC MISC
kunena -- kunena	Kunena before 5.0.4 does not restrict avatar file extensions to gif, jpeg, jpg, and png. This can lead to XSS and remote code execution.	2020-02-25	4.3	CVE-2016-11020 MISC MISC MISC
litecart -- litecart	LiteCart through 2.2.1 allows admin/?app=users&doc=edit_user CSRF to add a user.	2020-02-25	5	CVE-2020-9018 MISC MISC
litecart -- litecart	LiteCart through 2.2.1 allows CSV injection via a customer's profile.	2020-02-25	6	CVE-2020-9017 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lua-openssl -- lua-openssl	openssl_x509_check_host in lua-openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non-boolean return values.	2020-02-27	6.4	CVE-2020-9432 MISC
lua-openssl -- lua-openssl	openssl_x509_check_email in lua-openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non-boolean return values.	2020-02-27	6.4	CVE-2020-9433 MISC
lua-openssl -- lua-openssl	openssl_x509_check_ip_asc in lua-openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non-boolean return values.	2020-02-27	6.4	CVE-2020-9434 MISC
mcafee -- web_advisor	Remote Code Execution vulnerability in the web interface in McAfee Web Advisor (WA) 8.0.34745 and earlier allows remote unauthenticated attacker to execute arbitrary code via a cross site scripting attack.	2020-02-24	4.3	CVE-2019-3670 CONFIRM
miele -- xgw_3000_zigbee_gateway	In MIELE XGW 3000 ZigBee Gateway before 2.4.0, a malicious website visited by an authenticated admin user or a malicious mail is allowed to make arbitrary changes in the "admin panel" because there is no CSRF protection.	2020-02-24	6.8	CVE-2019-20480 MISC
miele -- xgw_300_zigbee_gateway	In MIELE XGW 3000 ZigBee Gateway before 2.4.0, the Password Change Function does not require knowledge of the old password. This can be exploited in conjunction with CVE-2019-20480.	2020-02-24	5	CVE-2019-20481 MISC
moxa -- awk-3131a_devices	The usage of hard-coded cryptographic keys within the ServiceAgent binary allows for the decryption of captured traffic across the network from or to the Moxa AWK-3131A firmware version 1.13.	2020-02-25	5	CVE-2019-5137 MISC
moxa -- awk-3131a_devices	An exploitable denial-of-service vulnerability exists in ServiceAgent functionality of the Moxa AWK-3131A, firmware version 1.13. A specially crafted packet can cause an integer underflow, triggering a large memcpy that will access unmapped or out-of-bounds memory. An attacker can send this packet while unauthenticated to trigger this vulnerability.	2020-02-25	5	CVE-2019-5148 MISC
moxa -- awk-3131a_devices	An exploitable command injection vulnerability exists in the iwwebs functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted diagnostic script file name can cause user input to be reflected in a subsequent iwsystem call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2020-02-25	6.5	CVE-2019-5140 MISC
moxa -- awk-3131a_devices	An exploitable format string vulnerability exists in the iw_console conio_writestr functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted time server entry can cause an overflow of the time server buffer, resulting in remote code	2020-02-25	6.5	CVE-2019-5143 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.			
moxa -- awk-3131a_devices	An exploitable command injection vulnerability exists in the iw_webs functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted iw_serverip parameter can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2020-02-25	6.5	CVE-2019-5141 MISC
moxa -- awk-3131a_devices	An exploitable remote code execution vulnerability exists in the iw_webs configuration parsing functionality of the Moxa AWK-3131A firmware version 1.13. A specially crafted user name entry can cause an overflow of an error message buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2020-02-25	6.5	CVE-2019-5153 MISC
moxa -- awk-3131a_devices	An exploitable authentication bypass vulnerability exists in the hostname processing of the Moxa AWK-3131A firmware version 1.13. A specially configured device hostname can cause the device to interpret select remote traffic as local traffic, resulting in a bypass of web authentication. An attacker can send authenticated SNMP requests to trigger this vulnerability.	2020-02-25	6.5	CVE-2019-5165 MISC
netgear -- nighthawk_x10-r900_devices	In NETGEAR Nighthawk X10-R900 prior to 1.0.4.26, an attacker may bypass all authentication checks on the device's "NETGEAR Genie" SOAP API ("/soap/server_sa") by supplying a malicious X-Forwarded-For header of the device's LAN IP address (192.168.1.1) in every request. As a result, an attacker may modify almost all of the device's settings and view various configuration settings.	2020-02-24	6.4	CVE-2019-12510 MISC
netgear -- nighthawk_x10-r900_devices	In NETGEAR Nighthawk X10-R900 prior to 1.0.4.24, by sending a DHCP discover request containing a malicious hostname field, an attacker may execute stored XSS attacks against this device. When the malicious DHCP request is received, the device will generate a log entry containing the malicious hostname. This log entry may then be viewed at Advanced settings->Administration->Logs to trigger the exploit. Although this value is inserted into a textarea tag, converted to all-caps, and limited in length, attacks are still possible.	2020-02-24	4.3	CVE-2019-12513 MISC
netgear -- nighthawk_x10-r900_devices	In NETGEAR Nighthawk X10-R900 prior to 1.0.4.24, an attacker may execute stored XSS attacks against this device by supplying a malicious X-Forwarded-For header while performing an incorrect login attempt. The value supplied by this header will be inserted into administrative logs, found at Advanced settings->Administration->Logs, and may trigger when the page is viewed. Although this value is inserted into a textarea tag, the attack simply needs to supply a closing textarea tag.	2020-02-24	4.3	CVE-2019-12512 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-xchange -- ox_app_suite_and_ox_documents	OX App Suite through 7.10.2 allows SSRF.	2020-02-21	4	CVE-2019-18846 MISC
opensmtpd -- opensmtpd	OpenSMTPD before 6.6.4 allows local users to read arbitrary files (e.g., on some Linux distributions) because of a combination of an untrusted search path in makemap.c and race conditions in the offline functionality in smtpd.c.	2020-02-25	4.7	CVE-2020-8793 FULLDISC MLIST MISC
otrs -- open_ticket_request_system	Kernel/Modules/AgentTicketPhone.pm in Open Ticket Request System (OTRS) 3.0.x before 3.0.20, 3.1.x before 3.1.16, and 3.2.x before 3.2.7, and OTRS ITSM 3.0.x before 3.0.8, 3.1.x before 3.1.9, and 3.2.x before 3.2.5 does not properly restrict tickets, which allows remote attackers with a valid agent login to read restricted tickets via a crafted URL involving the ticket split mechanism.	2020-02-21	4	CVE-2013-3551 MISC MISC
otrs -- open_ticket_request_system	Kernel/Modules/AgentTicketWatcher.pm in Open Ticket Request System (OTRS) 3.0.x before 3.0.21, 3.1.x before 3.1.17, and 3.2.x before 3.2.8 does not properly restrict tickets, which allows remote attackers with a valid agent login to read restricted tickets via a crafted URL involving the ticket split mechanism.	2020-02-21	4	CVE-2013-4088 MISC MISC MISC MISC
pacman -- pacman	pacman before 5.2 is vulnerable to arbitrary command injection in lib/libalpm/sync.c in the apply_deltas() function. This can be exploited when unsigned databases are used. To exploit the vulnerability, the user must enable the non-default delta feature and retrieve an attacker-controlled crafted database and delta file.	2020-02-24	6.8	CVE-2019-18183 MISC MISC MISC
pacman -- pacman	pacman before 5.2 is vulnerable to arbitrary command injection in conf.c in the download_with_xfercommand() function. This can be exploited when unsigned databases are used. To exploit the vulnerability, the user must enable a non-default XferCommand and retrieve an attacker-controlled crafted database and package.	2020-02-24	6.8	CVE-2019-18182 MISC MISC CONFIRM
php -- php	In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, certain content inside PHAR file could lead to one-byte read past the allocated buffer. This could potentially lead to information disclosure or crash.	2020-02-27	6.4	CVE-2020-7061 MISC
php -- php	In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash.	2020-02-27	4.3	CVE-2020-7062 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
php -- php	In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator() function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.	2020-02-27	5	CVE-2020-7063 MISC
pure-ftpd -- pure-ftpd	An issue was discovered in Pure-FTPd 1.0.49. An out-of-bounds (OOB) read has been detected in the pure_strcmp function in utils.c.	2020-02-24	5	CVE-2020-9365 MISC
rpi -- rpi	rpi through 0.0.3 allows execution of arbitrary commands. The variable pinNumbver in function GPIO within src/lib/gpio.js is used as part of the arguement of exec function without any sanitization.	2020-02-24	6.8	CVE-2019-10796 MISC MISC
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. A user with valid credentials is able to read XML files on the filesystem via the web interface. The PHP page /common/vam_editXml.php doesn't check the parameter that identifies the file name to be read. Thus, an attacker can manipulate the file name to access a potentially sensitive file within the filesystem.	2020-02-26	4	CVE-2019-19992 MISC MISC MISC
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. Several full path disclosure vulnerability were discovered. A user, even with no authentication, may simply send arbitrary content to the vulnerable pages to generate error messages that expose some full paths.	2020-02-26	5	CVE-2019-19993 MISC MISC MISC
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. It allows Cross-Site Request Forgery (CSRF) on any HTML form. An attacker can exploit the vulnerability to abuse functionalities such as change password, add user, add privilege, and so on.	2020-02-26	4.3	CVE-2019-19987 MISC MISC MISC
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. Several PHP pages, and other type of files, are reachable by any user without checking for user identity and authorization.	2020-02-26	5	CVE-2019-19989 MISC MISC MISC
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. A user with valid credentials is able to create and write XML files on the filesystem via /common/vam_editXml.php in the web interface. The vulnerable PHP page checks none of these: the parameter that identifies the file name to be created, the destination path, or the extension. Thus, an attacker can manipulate the file name to create any type of file within the filesystem with arbitrary content.	2020-02-26	6.5	CVE-2019-19988 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. An attacker without authentication is able to execute arbitrary SQL SELECT statements by injecting the HTTP (POST or GET) parameter persoid into /tools/VamPersonPhoto.php. The SQL Injection type is Error-based (this means that relies on error messages thrown by the database server to obtain information about the structure of the database).	2020-02-26	5	CVE-2019-19986 MISC MISC MISC
smartclient -- smartclient	An issue was discovered in SmartClient 12.0. The Remote Procedure Call (RPC) saveFile provided by the console functionality on the /tools/developerConsoleOperations.jsp (or /isomorphic/IDACall) URL allows an unauthenticated attacker to overwrite files via vectors involving an XML comment and /.. path traversal.	2020-02-23	6.4	CVE-2020-9354 MISC
smartclient -- smartclient	An issue was discovered in SmartClient 12.0. The Remote Procedure Call (RPC) loadFile provided by the console functionality on the /tools/developerConsoleOperations.jsp (or /isomorphic/IDACall) URL is affected by unauthenticated Local File Inclusion via directory-traversal sequences in the elem XML element in the _transaction parameter.	2020-02-23	5	CVE-2020-9353 MISC
smartclient -- smartclient	An issue was discovered in SmartClient 12.0. If an unauthenticated attacker makes a POST request to /tools/developerConsoleOperations.jsp or /isomorphic/IDACall with malformed XML data in the _transaction parameter, the server replies with a verbose error showing where the application resides (the absolute path).	2020-02-23	5	CVE-2020-9351 MISC
sqlite -- sqlite	In SQLite 3.31.1, isAuxiliaryVtabOperator allows attackers to trigger a NULL pointer dereference and segmentation fault because of generated column optimizations.	2020-02-21	5	CVE-2020-9327 MISC MISC MISC
sympa-community -- sympa	Sympa 6.2.38 through 6.2.52 allows remote attackers to cause a denial of service (disk consumption from temporary files, and a flood of notifications to listmasters) via a series of requests with malformed parameters.	2020-02-24	5	CVE-2020-9369 MISC MISC
total.js -- cms	controllers/admin.js in Total.js CMS 13 allows remote attackers to execute arbitrary code via a POST to the /admin/api/widgets/ URI. This can be exploited in conjunction with CVE-2019-15954.	2020-02-24	5	CVE-2020-9381 MISC MISC
tucan -- tucan	Insecure plugin update mechanism in tucan through 0.3.10 could allow remote attackers to perform man-in-the-middle attacks and execute arbitrary code ith the permissions of the user running tucan.	2020-02-21	6.8	CVE-2012-0063 MLIST MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ua-parser -- uap-core	uap-core before 0.7.3 is vulnerable to a denial of service attack when processing crafted User-Agent strings. Some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This has been patched in uap-core 0.7.3.	2020-02-21	5	CVE-2020-5243 MISC CONFIRM
wireshark -- wireshark	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the EAP dissector could crash. This was addressed in epan/dissectors/packet-eap.c by using more careful sscanf parsing.	2020-02-27	5	CVE-2020-9428 MISC MISC MISC
wireshark -- wireshark	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the LTE RRC dissector could leak memory. This was addressed in epan/dissectors/packet-lte-rrc.c by adjusting certain append operations.	2020-02-27	5	CVE-2020-9431 MISC MISC MISC
wireshark -- wireshark	In Wireshark 3.2.0 to 3.2.1, the WireGuard dissector could crash. This was addressed in epan/dissectors/packet-wireguard.c by handling the situation where a certain data structure intentionally has a NULL value.	2020-02-27	5	CVE-2020-9429 MISC MISC MISC MISC
wireshark -- wireshark	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the WiMax DLMAP dissector could crash. This was addressed in plugins/epan/wimax/msg_dlmap.c by validating a length field.	2020-02-27	5	CVE-2020-9430 MISC MISC MISC MISC MISC
wordpress -- wordpress	The Hero Maps Premium plugin 2.2.1 and prior for WordPress is prone to unauthenticated XSS via the views/dashboard/index.php p parameter because it fails to sufficiently sanitize user-supplied input. An attacker may leverage this issue to inject HTML or arbitrary JavaScript within the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based tokens or to launch other attacks.	2020-02-26	4.3	CVE-2019-19134 MISC MISC MISC MISC
wordpress -- wordpress	includes/options.php in the motors-car-dealership-classified-listings (aka Motors - Car Dealer & Classified Ads) plugin through 1.4.0 for WordPress has multiple stored XSS issues.	2020-02-24	4.3	CVE-2019-17229 MISC MISC MISC
wordpress -- wordpress	The WPJobBoard plugin 5.5.3 for WordPress allows Persistent XSS via the Add Job form, as demonstrated by title and Description.	2020-02-25	4.3	CVE-2020-9019

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
wordpress -- wordpress	An issue was discovered in the pricing-table-by-supsystic plugin before 1.8.2 for WordPress. It allows XSS.	2020-02-25	4.3	CVE-2020-9393 MISC
wordpress -- wordpress	An issue was discovered in the pricing-table-by-supsystic plugin before 1.8.2 for WordPress. It allows CSRF.	2020-02-25	6.8	CVE-2020-9394 MISC
wordpress -- wordpress	includes/options.php in the motors-car-dealership-classified-listings (aka Motors - Car Dealer & Classified Ads) plugin through 1.4.0 for WordPress allows unauthenticated options changes.	2020-02-24	6.4	CVE-2019-17228 MISC MISC MISC
zint -- zint	A NULL Pointer Dereference exists in libzint in Zint 2.7.1 because multiple + characters are mishandled in add_on in upcean.c, when called from eanx in upcean.c during EAN barcode generation.	2020-02-25	5	CVE-2020-9385 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
blackboard -- learn	Stored Cross-site scripting (XSS) vulnerability in Blackboard Learn/PeopleTool v9.1 allows users to inject arbitrary web script via the Tile widget in the People Tool profile editor.	2020-02-25	3.5	CVE-2020-9008 MISC MISC
dnn_software -- dnn	DNN (formerly DotNetNuke) through 9.4.4 allows XSS (issue 1 of 2).	2020-02-24	3.5	CVE-2020-5186 MISC MISC MISC
election -- election	fauzantrif eLection 2.0 has XSS via the Admin Dashboard -> Settings -> Election -> "message if election is closed" field.	2020-02-22	3.5	CVE-2020-9336 MISC
fiserv -- accurate_reconciliation	Fiserv Accurate Reconciliation 2.19.0 allows XSS via the Source or Destination field of the Configuration Manager (Configuration Parameter Translation) page.	2020-02-26	3.5	CVE-2020-8951 MISC
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 and 10.5.0, when protecting Microsoft SQL or Microsoft Exchange, could allow an attacker with intimate knowledge of the system to obtain highly sensitive information.	2020-02-24	2.9	CVE-2019-4703 XF CONFIRM
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 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: 167879.	2020-02-26	3.5	CVE-2019-4596 XF CONFIRM
moxa -- awk_3131A_devices	An exploitable use of hard-coded credentials vulnerability exists in multiple iw_* utilities of the Moxa AWK-3131A firmware version 1.13. The device operating system contains an undocumented encryption password, allowing for the creation of custom diagnostic scripts.	2020-02-25	3.6	CVE-2019-5139 MISC
netsurf -- netsurf	Information-disclosure vulnerability in Netsurf through 2.8 due to a world-readable cookie jar.	2020-02-21	2.1	CVE-2012-0844 MISC MISC MISC BID
sas -- visual_analytics	Graph Builder in SAS Visual Analytics 8.5 allows XSS via a graph template that is accessed directly.	2020-02-23	3.5	CVE-2020-9350 MISC
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. Multiple Stored Cross-site scripting (XSS) vulnerabilities allow remote authenticated users to inject arbitrary web script or HTML via the web pages /monitor/s_headmodel.php and /vam/vam_user.php.	2020-02-26	3.5	CVE-2019-19990 MISC MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
selesta -- visual_access_manager	An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. Multiple Reflected Cross-site scripting (XSS) vulnerabilities allow remote authenticated users to inject arbitrary web script or HTML via the web pages /vam/vam_anagraphic.php, /vam/vam_vamuser.php, /common/vamp_main.php, and /wiz/change_password.php.	2020-02-26	3.5	CVE-2019-19991 MISC MISC MISC
soplanning -- simple_online_planning	SOPlanning 1.45 allows XSS via the "Your SoPlanning url" field.	2020-02-22	3.5	CVE-2020-9338 MISC
soplanning -- simple_online_planning	SOPlanning 1.45 allows XSS via the Name or Comment to status.php.	2020-02-22	3.5	CVE-2020-9339 MISC
wordpress -- wordpress	A stored XSS vulnerability exists in the Envira Photo Gallery plugin through 1.7.6 for WordPress. Successful exploitation of this vulnerability would allow a authenticated low-privileged user to inject arbitrary JavaScript code that is viewed by other users.	2020-02-25	3.5	CVE-2020-9334 MISC MISC
wordpress -- wordpress	Multiple stored XSS vulnerabilities exist in the 10Web Photo Gallery plugin before 1.5.46 WordPress. Successful exploitation of this vulnerability would allow a authenticated admin user to inject arbitrary JavaScript code that is viewed by other users.	2020-02-25	3.5	CVE-2020-9335 MISC MISC