BULLETIN (SB21-123)

VULNERABILITY SUMMARY FOR THE WEEK OF

26TH APRIL, 2021

Bulletin (SB21-123)
Vulnerability Summary for the Week of April 26, 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
avaya -- session_border_controller_for_enterprise	A command injection vulnerability in Avaya Session Border Controller for Enterprise could allow an authenticated, remote attacker to send specially crafted messages and execute arbitrary commands with the affected system privileges. Affected versions of Avaya Session Border Controller for Enterprise include 7.x, 8.0 through 8.1.1.x	2021-04-23	9	CVE-2020-7034 CONFIRM
ibm -- spectrum_protect_backup-archive_client	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 could allow a local user to escalate their privileges to take full control of the system due to insecure directory permissions. IBM X-Force ID: 198811.	2021-04-26	7.2	CVE-2021-20532 CONFIRM XF
ibm -- spectrum_protect_client	IBM Spectrum Protect Client 8.1.0.0-8 through 1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing the current locale settings. A local attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges or cause the application to crash. IBM X-Force ID: 199479	2021-04-26	7.2	CVE-2021-29672 CONFIRM XF
inxedu -- inxedu	SQL Injection in com/inxedu/OS/edu/controller/letter/AdminMsgSystemController in Inxedu v2.0.6 via the ids parameter to admin/letter/delsystem.	2021-04-29	7.5	CVE-2020-35430 MISC
jquery-bbq_project -- jquery-bbq	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-bbq 1.2.1 allows a malicious user to inject properties into Object.prototype.	2021-04-23	7.5	CVE-2021-20086 MISC
manta -- safe-obj	Prototype pollution vulnerability in 'safe-obj' versions 1.0.0 through 1.0.2 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-04-26	7.5	CVE-2021-25928 MISC MISC
nec -- aterm_wg2600hs_firmware	Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors.	2021-04-26	10	CVE-2021-20711 MISC MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in the regional allocator via regional_alloc.	2021-04-27	7.5	CVE-2019-25032 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in the regional allocator via the ALIGN_UP macro.	2021-04-27	7.5	CVE-2019-25033 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in sldns_str2wire_dname_buf_origin, leading to an out-of-bounds write.	2021-04-27	7.5	CVE-2019-25034 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an out-of-bounds write in sldns_bget_token_par.	2021-04-27	7.5	CVE-2019-25035 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in a size calculation in dnscrypt/dnscrypt.c.	2021-04-27	7.5	CVE-2019-25038 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in a size calculation in respip/respip.c.	2021-04-27	7.5	CVE-2019-25039 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an out-of-bounds write via a compressed name in rdata_copy.	2021-04-27	7.5	CVE-2019-25042 MISC

HIGH Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pulsesecure -- pulse_connect_secure	Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been exploited in the wild.	2021-04-23	7.5	CVE-2021-22893 MISC MISC MISC MISC
purl_project -- purl	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in purl 2.3.2 allows a malicious user to inject properties into Object.prototype.	2021-04-23	7.5	CVE-2021-20089 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acemetrix -- jquery-deparam	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-deparam 0.5.1 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20087 MISC
aterm -- wg2600hs_firmware	Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.5.1 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-04-26	4.3	CVE-2021-20710 MISC MISC
avaya -- aura_orchestration_designer	An XML External Entities (XXE)vulnerability in the web-based user interface of Avaya Aura Orchestration Designer could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Orchestration Designer includes all 7.x versions before 7.2.3.	2021-04-23	4	CVE-2020-7035 CONFIRM
avaya -- callback_assist	An XML External Entities (XXE)vulnerability in Callback Assist could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Callback Assist includes all 4.0.x versions before 4.7.1.1 Patch 7.	2021-04-23	4	CVE-2020-7036 CONFIRM
backbone-query-parameters_project -- backbone-query-parameters	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in backbone-query-parameters 0.4.0 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20085 MISC
criticalmanufacturing -- cncsoft-b	CNCSoft-B Versions 1.0.0.3 and prior is vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code.	2021-04-27	6.8	CVE-2021-22664 MISC MISC
directum -- directum	Settings.aspx?view=About in Directum 5.8.2 allows XSS via the HTTP User-Agent header.	2021-04-24	4.3	CVE-2021-31794 MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.	2021-04-23	6.5	CVE-2021-22205 MISC MISC CONFIRM
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21227 MISC MISC GENTOO
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21230 MISC MISC GENTOO
google -- chrome	Use after free in Dev Tools in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21232 MISC MISC GENTOO
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21224 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				DEBIAN GENTOO
google -- chrome	Integer overflow in Mojo in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21223 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in Blink in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21206 MISC MISC GENTOO
google -- chrome	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21220 MISC MISC GENTOO
google -- chrome	Use after free in WebMIDI in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21213 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in IndexedDB in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2021-04-26	6.8	CVE-2021-21207 MISC MISC DEBIAN GENTOO
google -- chrome	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21233 MISC MISC GENTOO
google -- chrome	Use after free in Blink in Google Chrome on OS X prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21204 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in Blink in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21203 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in navigation in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21226 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				DEBIAN GENTOO
google -- chrome	Use after free in Network API in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.	2021-04-26	6.8	CVE-2021-21214 MISC MISC DEBIAN GENTOO
google -- chrome	Out of bounds memory access in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21225 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in permissions in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21201 MISC MISC DEBIAN GENTOO
google -- chrome	Incorrect security UI in Network Config UI in Google Chrome on ChromeOS prior to 90.0.4430.72 allowed a remote attacker to potentially compromise WiFi connection security via a malicious WAP.	2021-04-26	4.3	CVE-2021-21212 MISC MISC DEBIAN GENTOO
google -- chrome	Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21222 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in storage in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21209 MISC MISC DEBIAN GENTOO
google -- chrome	Insufficient policy enforcement in navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-04-26	5.8	CVE-2021-21205 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2021-04-26	6.8	CVE-2021-21202 MISC MISC DEBIAN GENTOO

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient data validation in QR scanner in Google Chrome on iOS prior to 90.0.4430.72 allowed an attacker displaying a QR code to perform domain spoofing via a crafted QR code.	2021-04-26	4.3	CVE-2021-21208 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Network in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially access local UDP ports via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21210 MISC MISC DEBIAN GENTOO
google -- chrome	Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21221 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21211 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21215 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21216 MISC MISC DEBIAN GENTOO
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-04-26	4.3	CVE-2021-21217 MISC MISC DEBIAN GENTOO
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-04-26	4.3	CVE-2021-21218 MISC MISC DEBIAN GENTOO
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-04-26	4.3	CVE-2021-21219 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				DEBIAN GENTOO
hornerautomation -- cscape	Cscape (All versions prior to 9.90 SP4) lacks proper validation of user-supplied data when parsing project files. This could lead to memory corruption. An attacker could leverage this vulnerability to execute code in the context of the current process.	2021-04-23	6.8	CVE-2021-22678 MISC
hornerautomation -- cscape	Cscape (All versions prior to 9.90 SP4) is configured by default to be installed for all users, which allows full permissions, including read/write access. This may allow unprivileged users to modify the binaries and configuration files and lead to local privilege escalation.	2021-04-23	4.6	CVE-2021-22682 MISC
ibm -- informix_dynamic_server	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366.	2021-04-30	4.6	CVE-2021-20515 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information by allowing cross-window communication with unrestricted target origin via documentation frames.	2021-04-26	5	CVE-2020-4562 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 200258.	2021-04-26	5	CVE-2021-29694 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 196344.	2021-04-26	6.4	CVE-2021-20432 XF CONFIRM
jamovi -- jamovi	Jamovi <=1.6.18 is affected by a cross-site scripting (XSS) vulnerability. The column-name is vulnerable to XSS in the ElectronJS Framework. An attacker can make a .omv (Jamovi) document containing a payload. When opened by victim, the payload is triggered.	2021-04-26	4.3	CVE-2021-28079 MISC MISC
jquery-plugin-query-object_project -- jquery-plugin-query-object	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-plugin-query-object 2.2.3 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20083 MISC
jquery-sparkle_project -- jquery-sparkle	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-sparkle 1.5.2-beta allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20084 MISC
minthcm -- minthcm	The Import function in MintHCM RELEASE 3.0.8 allows an attacker to execute a cross-site scripting (XSS) payload in file-upload.	2021-04-26	4.3	CVE-2021-25838 MISC MISC
mootools -- mootools-more	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in mootools-more 1.6.0 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20088 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an assertion failure and denial of service in synth_cname.	2021-04-27	5	CVE-2019-25036 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an assertion failure and denial of service in dname_pkt_copy via an invalid packet.	2021-04-27	5	CVE-2019-25037 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nlnetlabs -- unbound	Unbound before 1.9.5 allows an infinite loop via a compressed name in dname_pkt_copy.	2021-04-27	5	CVE-2019-25040 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an assertion failure via a compressed name in dname_pkt_copy.	2021-04-27	5	CVE-2019-25041 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows configuration injection in create_unbound_ad_servers.sh upon a successful man-in-the-middle attack against a cleartext HTTP session.	2021-04-27	4.3	CVE-2019-25031 MISC
pfsense -- pfsense	pfSense 2.5.0 allows XSS via the services_wol_edit.php Description field.	2021-04-28	4.3	CVE-2021-27933 FULLDISC
webmin -- webmin	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to achieve Remote Command Execution (RCE) through Webmin's running process feature.	2021-04-25	6.8	CVE-2021-31760 MISC MISC MISC MISC
webmin -- webmin	Webmin 1.973 is affected by reflected Cross Site Scripting (XSS) to achieve Remote Command Execution through Webmin's running process feature.	2021-04-25	6.8	CVE-2021-31761 MISC MISC MISC MISC
webmin -- webmin	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to create a privileged user through Webmin's add users feature, and then get a reverse shell through Webmin's running process feature.	2021-04-25	6.8	CVE-2021-31762 MISC MISC MISC MISC
wireshark -- wireshark	Excessive memory consumption in MS-WSP dissector in Wireshark 3.4.0 to 3.4.4 and 3.2.0 to 3.2.12 allows denial of service via packet injection or crafted capture file	2021-04-23	5	CVE-2021-22207 CONFIRM MISC MISC
xmlhttprequest-ssl_project -- xmlhttprequest-ssl	The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected.	2021-04-23	5.8	CVE-2021-31597 MISC MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dotcms -- dotcms	Cross Site Scripting (XSS) in dotCMS v5.1.5 allows remote attackers to execute arbitrary code by injecting a malicious payload into the "Task Detail" comment window of the "/dotAdmin/#/c/workflow" component.	2021-04-23	3.5	CVE-2020-17542 MISC
ibm -- spectrum_protect_client	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and cause the application to crash. IBM X-Force ID: 198934	2021-04-26	2.1	CVE-2021-20546 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus File Systems Agent 10.1.6 and 10.1.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 198836.	2021-04-26	2.1	CVE-2021-20536 CONFIRM XF
vaadin -- flow	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.13 (Vaadin 10.0.0 through 10.0.16), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.4.6 (Vaadin 14.0.0 through 14.4.6), 3.0.0 prior to 5.0.0 (Vaadin 15 prior to 18), and 5.0.0 through 5.0.2 (Vaadin 18.0.0 through 18.0.5) allows attacker to guess a security token via timing attack.	2021-04-23	1.9	CVE-2021-31404 CONFIRM CONFIRM
vaadin -- flow	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server versions 3.0.0 through 5.0.3 (Vaadin 15.0.0 through 18.0.6), and com.vaadin:fusion-endpoint version 6.0.0 (Vaadin 19.0.0) allows attacker to guess a security token for Fusion endpoints via timing attack.	2021-04-23	1.9	CVE-2021-31406 CONFIRM CONFIRM
vaadin -- vaadin	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:vaadin-server versions 7.0.0 through 7.7.23 (Vaadin 7.0.0 through 7.7.23), and 8.0.0 through 8.12.2 (Vaadin 8.0.0 through 8.12.2) allows attacker to guess a security token via timing attack	2021-04-23	1.9	CVE-2021-31403 CONFIRM CONFIRM CONFIRM
wowza -- streaming_engine	Wowza Streaming Engine through 4.8.5 (in a default installation) has incorrect file permissions of configuration files in the conf/ directory. A regular local user is able to read and write to all the configuration files, e.g., modify the application server configuration.	2021-04-23	3.6	CVE-2021-31540 MISC MISC
wowza -- streaming_engine	Wowza Streaming Engine through 4.8.5 (in a default installation) has cleartext passwords stored in the conf/admin.password file. A regular local user is able to read usernames and passwords.	2021-04-23	2.1	CVE-2021-31539 MISC MISC