الهيئة الوطنية للأمن السيبراني
Nat onal Cybersecurity Authority

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 30th of July to 5th of August. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٣٠ يوليو إلى ٥ اغسطس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-31710	tp-link - multiple products	TP-Link Archer AX21(US)_V3_1.1.4 Build 20230219 and AX21(US)_V3.6_1.1.4 Build 20230219 are vulnerable to Buffer Overflow.	2023-08-01	9.8	Critical
CVE-2023-4056	mozilla - multiple products	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	9.8	Critical
CVE-2023-4057	mozilla - multiple products	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, and Thunderbird 115.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1.	2023-08-01	9.8	Critical
CVE-2023-4058	mozilla - firefox	Memory safety bugs present in Firefox 115. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116.	2023-08-01	9.8	Critical
CVE-2022-40609	ibm - multiple products	IBM SDK, Java Technology Edition 7.1.5.18 and 8.0.8.0 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization flaw. By sending specially-crafted data, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236069.	2023-08-02	9.8	Critical
CVE-2023-20214	cisco - multiple products	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI.	2023-08-03	9.1	Critical
CVE-2023-35019	ibm - security_verify_governance	IBM Security Verify Governance, Identity Manager 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 257873.	2023-07-31	8.8	High
CVE-2023-4047	mozilla - multiple products	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	8.8	High

CVE-2023-3727	google - chrome	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-01	8.8	High
CVE-2023-3728	google - chrome	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-01	8.8	High
CVE-2023-3729	google - chrome	Use after free in Splitscreen in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. (Chromium security severity: High)	2023-08-01	8.8	High
CVE-2023-3730	google - chrome	Use after free in Tab Groups in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-01	8.8	High
CVE-2023-3731	google - chrome	Use after free in Diagnostics in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	2023-08-01	8.8	High
CVE-2023-3732	google - chrome	Out of bounds memory access in Mojo in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-01	8.8	High
CVE-2023-4069	google - chrome	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4071	google - chrome	Heap buffer overflow in Visuals in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4072	google - chrome	Out of bounds read and write in WebGL in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4073	google - chrome	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4074	google - chrome	Use after free in Blink Task Scheduling in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4075	google - chrome	Use after free in Cast in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4076	google - chrome	Use after free in WebRTC in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC session. (Chromium security severity: High)	2023-08-03	8.8	High
CVE-2023-4077	google - chrome	Insufficient data validation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)	2023-08-03	8.8	High
CVE-2023-4078	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)	2023-08-03	8.8	High
CVE-2023-29505	zohocorp - manageengine_network_configuration_manager	An issue was discovered in Zoho ManageEngine Network Configuration Manager 12.6.165. The WebSocket endpoint allows Cross-site WebSocket hijacking.	2023-08-04	8.8	High
CVE-2023-39508	apache - airflow	Execution with Unnecessary Privileges, : Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Airflow.The "Run Task" feature enables authenticated user to bypass some of the restrictions put in place. It allows to execute code in the webserver context as well as allows to bypas limitation of access the user has to certain DAGs. The "Run Task" feature is considered dangerous and it has been removed entirely in Airflow 2.6.0 This issue affects Apache Airflow: before 2.6.0.	2023-08-05	8.8	High
CVE-2023-4068	google - chrome	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.1	High

CVE-2023-4070	google - chrome	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-08-03	8.1	High
CVE-2020-26064	cisco - multiple products	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected system. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and write files within the affected application.	2023-08-04	8.1	High
CVE-2022-43831	ibm - spectrum_scale_container_native_storage_access	IBM Storage Scale Container Native Storage Access 5.1.2.1 through 5.1.6.1 could allow a local user to obtain escalated privileges on a host without proper security context settings configured. IBM X-Force ID: 238941.	2023-07-31	7.8	High
CVE-2023-4004	linux - multiple products	A use-after-free flaw was found in the Linux kernel's netfilter in the way a user triggers the nft_pipapo_remove function with the element, without a NFT_SET_EXT_KEY_END. This issue could allow a local user to crash the system or potentially escalate their privileges on the system.	2023-07-31	7.8	High
CVE-2023-38418	f5 - multiple products	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	7.8	High
CVE-2023-20216	cisco - multiple products	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability.	2023-08-03	7.8	High
CVE-2023-38750	zimbra - multiple products	In Zimbra Collaboration (ZCS) 8 before 8.8.15 Patch 41, 9 before 9.0.0 Patch 34, and 10 before 10.0.2, internal JSP and XML files can be exposed.	2023-07-31	7.5	High
CVE-2023-4048	mozilla - multiple products	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	7.5	High
CVE-2023-4050	mozilla - multiple products	In some cases, an untrusted input stream was copied to a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	7.5	High
CVE-2023-4051	mozilla - firefox	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 116.	2023-08-01	7.5	High
CVE-2023-4055	mozilla - multiple products	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	7.5	High
CVE-2023-35081	ivanti - multiple products	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows an authenticated administrator to write arbitrary files onto the appliance.	2023-08-03	7.2	High
CVE-2022-34453	dell - xtremio_x2_firmware	Dell XtremIO X2 XMS versions prior to 6-4-1.11 contain an improper access control vulnerability. A remote read only user could potentially exploit this vulnerability to perform add/delete QoS policies which are disabled by default.	2023-08-03	7.1	High
CVE-2023-35016	ibm - security_verify_governance	IBM Security Verify Governance, Identity Manager 10.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257772.	2023-07-31	6.5	Medium

CVE-2023-24971	ibm - multiple products	IBM B2B Advanced Communications 1.0.0.0 and IBM Multi-Enterprise Integration Gateway 1.0.0.1 could allow a user to cause a denial of service due to the deserializing of untrusted serialized Java objects. IBM X-Force ID: 246976.	2023-07-31	6.5	Medium
CVE-2023-4052	mozilla - multiple products	The Firefox updater created a directory writable by non-privileged users. When uninstalling Firefox, any files in that directory would be recursively deleted with the permissions of the uninstalling user account. This could be combined with creation of a junction (a form of symbolic link) to allow arbitrary file deletion controlled by the non-privileged user. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1.	2023-08-01	6.5	Medium
CVE-2023-4053	mozilla - firefox	A website could have obscured the full screen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 116.	2023-08-01	6.5	Medium
CVE-2023-23476	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7.latest is vulnerable to unauthorized access to data due to insufficient authorization validation on some API routes. IBM X-Force ID: 245425.	2023-08-02	6.5	Medium
CVE-2023-38332	zohocorp - multiple products	Zoho ManageEngine ADManager Plus through 7201 allow authenticated users to take over another user's account via sensitive information disclosure.	2023-08-04	6.5	Medium
CVE-2022-4955	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-08-04	6.5	Medium
CVE-2020-26065	cisco - multiple products	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system.	2023-08-04	6.5	Medium
CVE-2023-3739	google - chrome	Insufficient validation of untrusted input in Chromad in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker to execute arbitrary code via a crafted shell script. (Chromium security severity: Low)	2023-08-01	6.3	Medium
CVE-2023-37580	zimbra - multiple products	Zimbra Collaboration (ZCS) 8 before 8.8.15 Patch 41 allows XSS in the Zimbra Classic Web Client.	2023-07-31	6.1	Medium
CVE-2023-38138	f5 - multiple products	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	6.1	Medium
CVE-2023-3470	f5 - multiple products	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	6.1	Medium
CVE-2023-20181	cisco - spa500ds_firmware	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input	2023-08-03	6.1	Medium

		by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.			
CVE-2023-20218	cisco - spa500ds_firmware	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]]	2023-08-03	6.1	Medium
CVE-2023-30958	zabbix - frontend	A security defect was identified in Foundry Frontend that enabled users to potentially conduct DOM XSS attacks if Foundry's CSP were to be bypassed. This defect was resolved with the release of Foundry Frontend 6.225.0.	2023-08-03	6.1	Medium
CVE-2023-4049	mozilla - multiple products	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	5.9	Medium
CVE-2023-4054	mozilla - multiple products	When opening appref-ms files, Firefox did not warn the user that these files may contain malicious code. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 102.14, Firefox ESR < 115.1, Thunderbird < 102.14, and Thunderbird < 115.1.	2023-08-01	5.5	Medium
CVE-2023-36858	f5 - multiple products	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	5.5	Medium
CVE-2023-4132	linux - linux_kernel	A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition.	2023-08-03	5.5	Medium
CVE-2023-4133	linux - linux_kernel	A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs when the cxgb4 device is detaching due to a possible rearming of the flower_stats_timer from the work queue. This flaw allows a local user to crash the system, causing a denial of service condition.	2023-08-03	5.5	Medium
CVE-2023-22595	ibm - multiple products	IBM B2B Advanced Communications 1.0.0.0 and IBM Multi-Enterprise Integration Gateway 1.0.0.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244076.	2023-07-31	5.4	Medium
CVE-2023-38423	f5 - multiple products	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	5.4	Medium
CVE-2023-20204	cisco - multiple products	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to	2023-08-03	5.4	Medium

		execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.			
CVE-2020-4868	ibm - tririga_application_platform	IBM TRIRIGA 3.0, 4.0, and 4.4 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: 190744.	2023-07-31	5.3	Medium
CVE-2023-3817	openssl - multiple products	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.	2023-07-31	5.3	Medium
CVE-2023-4045	mozilla - multiple products	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	5.3	Medium
CVE-2023-4046	mozilla - multiple products	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis. This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	2023-08-01	5.3	Medium
CVE-2023-20215	cisco - multiple products	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device.	2023-08-03	5.3	Medium
CVE-2023-34037	vmware - multiple products	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests.	2023-08-04	5.3	Medium
CVE-2023-34038	vmware - multiple products	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration.	2023-08-04	5.3	Medium
CVE-2020-26082	cisco - asyncos	A vulnerability in the zip decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass content filters that	2023-08-04	5.3	Medium

		are configured on an affected device. The vulnerability is due to improper handling of password-protected zip files. An attacker could exploit this vulnerability by sending a malicious file inside a crafted zip-compressed file to an affected device. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email.			
CVE-2023-4010	linux - linux_kernel	A flaw was found in the USB Host Controller Driver framework in the Linux kernel. The usb_giveback_urb function has a logic loophole in its implementation. Due to the inappropriate judgment condition of the goto statement, the function cannot return under the input of a specific malformed descriptor file, so it falls into an endless loop, resulting in a denial of service.	2023-07-31	4.6	Medium
CVE-2023-36494	f5 - f5os-a	Audit logs on F5OS-A may contain undisclosed sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	4.4	Medium
CVE-2023-3733	google - chrome	Inappropriate implementation in WebApp Installs in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	2023-08-01	4.3	Medium
CVE-2023-3734	google - chrome	Inappropriate implementation in Picture In Picture in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	2023-08-01	4.3	Medium
CVE-2023-3735	google - chrome	Inappropriate implementation in Web API Permission Prompts in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-08-01	4.3	Medium
CVE-2023-3736	google - chrome	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 115.0.5790.98 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2023-08-01	4.3	Medium
CVE-2023-3737	google - chrome	Inappropriate implementation in Notifications in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to spoof the contents of media notifications via a crafted HTML page. (Chromium security severity: Medium)	2023-08-01	4.3	Medium
CVE-2023-3738	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-08-01	4.3	Medium
CVE-2023-3740	google - chrome	Insufficient validation of untrusted input in Themes in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially serve malicious content to a user via a crafted background URL. (Chromium security severity: Low)	2023-08-01	4.3	Medium
CVE-2023-3426	liferay - multiple products	The organization selector in Liferay Portal 7.4.3.81 through 7.4.3.85, and Liferay DXP 7.4 update 81 through 85 does not check user permission, which allows remote authenticated users to obtain a list of all organizations.	2023-08-02	4.3	Medium
CVE-2023-38419	f5 - multiple products	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-08-02	4.3	Medium

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.