الهيئـــة الوطنيـــة
للأمـــن السيبـــرانى
National 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 20th of August to 26th 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 ٢٠ أغسطس إلى ٢٦ أغسطس. 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-2023-39747	tp-link - tl-wr940n_v2_firmware	TP-Link WR841N V8, TP-Link TL-WR940N V2, and TL-WR941ND V5 were discovered to contain a buffer overflow via the radiusSecret parameter at /userRpm/WlanSecurityRpm.	2023-08-21	9.8	Critical
CVE-2023-39751	tp-link - tl-wr941nd_v6_firmware	TP-Link TL-WR941ND V6 were discovered to contain a buffer overflow via the pSize parameter at /userRpm/PingIframeRpm.	2023-08-21	9.8	Critical
CVE-2023-31447	draytek - vigor2620_firmware	user_login.cgi on Draytek Vigor2620 devices before 3.9.8.4 (and on all versions of Vigor2925 devices) allows attackers to send a crafted payload to modify the content of the code segment, insert shellcode, and execute arbitrary code.	2023-08-21	9.8	Critical
CVE-2023-38035	ivanti - mobileiron_sentry	A security vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry versions 9.18.0 and below, which may allow an attacker to bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration.	2023-08-21	9.8	Critical
CVE-2020-35357	gnu - multiple products	A buffer overflow can occur when calculating the quantile value using the Statistics Library of GSL (GNU Scientific Library), versions 2.5 and 2.6. Processing a maliciously crafted input data for gsl_stats_quantile_from_sorted_data of the library may lead to unexpected application termination or arbitrary code execution.	2023-08-22	9.8	Critical
CVE-2023-38734	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7.1 and 23.0.0 through 23.0.1 is vulnerable to incorrect privilege assignment when importing users from an LDAP directory. IBM X-Force ID: 262481.	2023-08-22	9.8	Critical
CVE-2019-13690	google - chrome	Inappropriate implementation in OS in Google Chrome on ChromeOS prior to 75.0.3770.80 allowed a remote attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High)	2023-08-25	9.6	Critical
CVE-2023-36787	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-08-21	8.8	High
CVE-2020-19726	gnu - binutils	An issue was discovered in binutils libbfd.c 2.36 relating to the auxiliary symbol data allows attackers to read or write to system memory or cause a denial of service.	2023-08-22	8.8	High
CVE-2023-4429	google - chrome	Use after free in Loader in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-23	8.8	High
CVE-2023-4430	google - chrome	Use after free in Vulkan in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-23	8.8	High
CVE-2022-46884	mozilla - firefox	A potential use-after-free vulnerability existed in SVG Images if the Refresh Driver was destroyed at an inopportune time. This could have lead to memory corruption or a potentially exploitable crash. *Note*: This advisory was added on December 13th, 2022 after discovering it was inadvertently left out of the original advisory. The fix was included in the original release of Firefox 106. This vulnerability affects Firefox < 106.	2023-08-24	8.8	High
CVE-2023-34971	qnap - multiple products	An inadequate encryption strength vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability	2023-08-24	8.8	High

		possibly allows local network clients to decrypt the data using brute force attacks via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later QuTS hero h5.1.0.2424 build 20230609 and later QuTS hero h4.5.4.2476 build 20230728 and later			
CVE-2022-4452	google - chrome	Insufficient data validation in crosvm in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-25	8.8	High
CVE-2022-46751	apache - ivy	Improper Restriction of XML External Entity Reference, XML Injection (aka Blind XPath Injection) vulnerability in Apache Software Foundation Apache Ivy.This issue affects any version of Apache Ivy prior to 2.5.2. When Apache Ivy prior to 2.5.2 parses XML files - either its own configuration, Ivy files or Apache Maven POMs - it will allow downloading external document type definitions and expand any entity references contained therein when used. This can be used to exfiltrate data, access resources only the machine running Ivy has access to or disturb the execution of Ivy in different ways. Starting with Ivy 2.5.2 DTD processing is disabled by default except when parsing Maven POMs where the default is to allow DTD processing but only to include a DTD snippet shipping with Ivy that is needed to deal with existing Maven POMs that are not valid XML files but are nevertheless accepted by Maven. Access can be be made more lenient via newly introduced system properties where needed. Users of Ivy prior to version 2.5.2 can use Java system properties to restrict processing of external DTDs, see the section about "JAXP Properties for External Access restrictions" inside Oracle's "Java API for XML Processing (JAXP) Security Guide".	2023-08-21	8.2	High
CVE-2023-37424	arubanetworks - multiple products	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host if certain preconditions outside of the attacker's control are met. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise.	2023-08-22	8.1	High
CVE-2023-37429	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	8.1	High
CVE-2023-37430	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	8.1	High
CVE-2023-37431	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	8.1	High
CVE-2023-37432	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the	2023-08-22	8.1	High

		underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.			
CVE-2023-37433	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	8.1	High
CVE-2023-37434	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	8.1	High
CVE-2023-4427	google - chrome	Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2023-08-23	8.1	High
CVE-2023-4428	google - chrome	Out of bounds memory access in CSS in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2023-08-23	8.1	High
CVE-2023-4431	google - chrome	Out of bounds memory access in Fonts in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2023-08-23	8.1	High
CVE-2023-37379	apache - airflow	Apache Airflow, in versions prior to 2.7.0, contains a security vulnerability that can be exploited by an authenticated user possessing Connection edit privileges. This vulnerability allows the user to access connection information and exploit the test connection feature by sending many requests, leading to a denial of service (DoS) condition on the server. Furthermore, malicious actors can leverage this vulnerability to establish harmful connections with the server. Users of Apache Airflow are strongly advised to upgrade to version 2.7.0 or newer to mitigate the risk associated with this vulnerability. Additionally, administrators are encouraged to review and adjust user permissions to restrict access to sensitive functionalities, reducing the attack surface.	2023-08-23	8.1	High
CVE-2023-40273	apache - airflow	The session fixation vulnerability allowed the authenticated user to continue accessing Airflow webserver even after the password of the user has been reset by the admin - up until the expiry of the session of the user. Other than manually cleaning the session database (for database session backend), or changing the secure_key and restarting the webserver, there were no mechanisms to force-logout the user (and all other users with that). With this fix implemented, when using the database session backend, the existing sessions of the user are invalidated when the password of the user is reset. When using the securecookie session backend, the sessions are NOT invalidated and still require changing the secure key and restarting the webserver (and logging out all other users), but the user resetting the password is informed about it with a flash message warning displayed in the UI. Documentation is also updated explaining this behaviour. Users of Apache Airflow are advised to upgrade to version 2.7.0 or newer to mitigate the risk associated with this vulnerability.	2023-08-23	8	High
CVE-2020-19725	microsoft - z3	There is a use-after-free vulnerability in file pdd_simplifier.cpp in Z3 before 4.8.8. It occurs when the solver attempt to simplify the constraints and causes unexpected memory access. It can cause segmentation faults or arbitrary code execution.	2023-08-22	7.8	High
CVE-2022-44840	gnu - binutils	Heap buffer overflow vulnerability in binutils readelf before 2.40 via function find_section_in_set in file readelf.c.	2023-08-22	7.8	High
CVE-2022-45703	gnu - binutils	Heap buffer overflow vulnerability in binutils readelf before 2.40 via function display_debug_section in file readelf.c.	2023-08-22	7.8	High
CVE-2022-47673	gnu - binutils	An issue was discovered in Binutils addr2line before 2.39.3, function parse_module contains multiple out of bound reads which may cause a denial of service or other unspecified impacts.	2023-08-22	7.8	High

CVE-2022-47695	gnu - binutils	An issue was discovered Binutils objdump before 2.39.3 allows attackers to cause a denial of service or other unspecified impacts via function bfd_mach_o_get_synthetic_symtab in match-o.c.	2023-08-22	7.8	High
CVE-2022-47696	gnu - binutils	An issue was discovered Binutils objdump before 2.39.3 allows attackers to cause a denial of service or other unspecified impacts via function compare_symbols.	2023-08-22	7.8	High
CVE-2023-3899	redhat - multiple products	A vulnerability was found in subscription-manager that allows local privilege escalation due to inadequate authorization. The D-Bus interface com.redhat.RHSM1 exposes a significant number of methods to all users that could change the state of the registration. By using the com.redhat.RHSM1.Config.SetAll() method, a low-privileged local user could tamper with the state of the registration, by unregistering the system or by changing the current entitlements. This flaw allows an attacker to set arbitrary configuration directives for /etc/rhsm/rhsm.conf, which can be abused to cause a local privilege escalation to an unconfined root.	2023-08-23	7.8	High
CVE-2023-34040	vmware - multiple products	In Spring for Apache Kafka 3.0.9 and earlier and versions 2.9.10 and earlier, a possible deserialization attack vector existed, but only if unusual configuration was applied. An attacker would have to construct a malicious serialized object in one of the deserialization exception record headers. Specifically, an application is vulnerable when all of the following are true: * The user does not configure an ErrorHandlingDeserializer for the key and/or value of the record * The user explicitly sets container properties checkDeserExWhenKeyNull and/or checkDeserExWhenValueNull container properties to true. * The user allows untrusted sources to publish to a Kafka topic By default, these properties are false, and the container only attempts to deserialize the headers if an ErrorHandlingDeserializer is configured. The ErrorHandlingDeserializer prevents the vulnerability by removing any such malicious headers before processing the record.	2023-08-24	7.8	High
CVE-2019-13689	google - chrome	Inappropriate implementation in OS in Google Chrome on ChromeOS prior to 75.0.3770.80 allowed a remote attacker to perform arbitrary read/write via a malicious file. (Chromium security severity: Critical)	2023-08-25	7.8	High
CVE-2023-39745	tp-link - tl-wr940n_v2_firmware	TP-Link TL-WR940N V2, TP-Link TL-WR941ND V5 and TP-Link TL-WR841N V8 were discovered to contain a buffer overflow via the component /userRpm/AccessCtrlAccessRulesRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-08-21	7.5	High
CVE-2023-39748	tp-link - tl-wr1041n_v2_firmware	An issue in the component /userRpm/NetworkCfgRpm of TP-Link TL-WR1041N V2 allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-08-21	7.5	High
CVE-2020-26652	realtek - rtl8812au_firmware	An issue was discovered in function nl80211_send_chandef in rtl8812au v5.6.4.2 allows attackers to cause a denial of service.	2023-08-22	7.5	High
CVE-2020-35342	gnu - binutils	GNU Binutils before 2.34 has an uninitialized-heap vulnerability in function tic4x_print_cond (file opcodes/tic4x-dis.c) which could allow attackers to make an information leak.	2023-08-22	7.5	High
CVE-2021-35309	samsung - syncthru_web_service	An issue discovered in Samsung SyncThru Web Service SPL 5.93 06-09-2014 allows attackers to gain escalated privileges via MITM attacks.	2023-08-22	7.5	High
CVE-2021-46174	gnu - binutils	Heap-based Buffer Overflow in function bfd_getl32 in Binutils objdump 3.37.	2023-08-22	7.5	High
CVE-2022-40433	oracle - multiple products	An issue was discovered in function ciMethodBlocks::make_block_at in Oracle JDK (HotSpot VM) 11, 17 and OpenJDK (HotSpot VM) 8, 11, 17, allows attackers to cause a denial of service.	2023-08-22	7.5	High
CVE-2023-37426	arubanetworks - multiple products	EdgeConnect SD-WAN Orchestrator instances prior to the versions resolved in this advisory were found to have shared static SSH host keys for all installations. This vulnerability could allow an attacker to spoof the SSH host signature and thereby masquerade as a legitimate Orchestrator host.	2023-08-22	7.5	High
CVE-2023-33850	ibm - multiple products	IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 257132.	2023-08-22	7.5	High

CVE-2023-1409	mongodb - multiple products	If the MongoDB Server running on Windows or macOS is configured to use TLS with a specific set of configuration options that are already known to work securely in other platforms (e.g. Linux), it is possible that client certificate validation may not be in effect, potentially allowing client to establish a TLS connection with the server that supplies any certificate. This issue affect all MongoDB Server v6.3 versions, MongoDB Server v5.0 versions v5.0.0 to v5.0.14 and all MongoDB Server v4.4 versions.	2023-08-23	7.5	High
CVE-2023-39289	mitel - mivoice_connect	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect through 9.6.2208.101 could allow an unauthenticated attacker to conduct an account enumeration attack due to improper configuration. A successful exploit could allow an attacker to access system information.	2023-08-25	7.5	High
CVE-2023-36741	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-08-26	7.5	High
CVE-2023-40352	mcafee - safe_connect	McAfee Safe Connect before 2.16.1.126 may allow an adversary with system privileges to achieve privilege escalation by loading arbitrary DLLs.	2023-08-21	7.2	High
CVE-2023-37427	arubanetworks - multiple products	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability allows an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-08-22	7.2	High
CVE-2023-37428	arubanetworks - multiple products	A vulnerability in the EdgeConnect SD-WAN Orchestrator web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-08-22	7.2	High
CVE-2022-44729	apache - xml_graphics_batik	Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache XML Graphics Batik.This issue affects Apache XML Graphics Batik: 1.16. On version 1.16, a malicious SVG could trigger loading external resources by default, causing resource consumption or in some cases even information disclosure. Users are recommended to upgrade to version 1.17 or later.	2023-08-22	7.1	High
CVE-2022-3742	lenovo - ideapad_1_14iau7_firmware	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to execute arbitrary code due to improper buffer validation.	2023-08-23	6.7	Medium
CVE-2022-3744	lenovo - ideapad_1_14iau7_firmware	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to unlock UEFI variables due to a hard-coded SMI handler credential.	2023-08-23	6.7	Medium
CVE-2022-3746	lenovo - ideapad_1_14iau7_firmware	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to cause some peripherals to work abnormally due to an exposed Embedded Controller (EC) interface.	2023-08-23	6.7	Medium
CVE-2023-4456	redhat - openshift_logging	A flaw was found in openshift-logging LokiStack. The key used for caching is just the token, which is too broad. This issue allows a user with a token valid for one action to execute other actions as long as the authorization allowing the original action is still cached.	2023-08-21	6.5	Medium
CVE-2023-38906	tp-link - multiple products	An issue in TPLink Smart bulb Tapo series L530 v.1.0.0 and Tapo Application v.2.8.14 allows a remote attacker to obtain sensitive information via the authentication code for the UDP message.	2023-08-22	6.5	Medium
CVE-2023-38908	tp-link - multiple products	An issue in TPLink Smart bulb Tapo series L530 v.1.0.0 and Tapo Application v.2.8.14 allows a remote attacker to obtain sensitive information via the TSKEP authentication function.	2023-08-22	6.5	Medium
CVE-2023-38909	tp-link - multiple products	An issue in TPLink Smart bulb Tapo series L530 v.1.0.0 and Tapo Application v.2.8.14 allows a remote attacker to obtain sensitive information via the IV component in the AES128-CBC function.	2023-08-22	6.5	Medium
CVE-2020-19185	gnu - ncurses	Buffer Overflow vulnerability in one_one_mapping function in progs/dump_entry.c:1373 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	2023-08-22	6.5	Medium
CVE-2020-19186	gnu - ncurses	Buffer Overflow vulnerability in _nc_find_entry function in tinfo/comp_hash.c:66 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	2023-08-22	6.5	Medium
CVE-2020-19187	gnu - ncurses	Buffer Overflow vulnerability in fmt_entry function in progs/dump_entry.c:1100 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	2023-08-22	6.5	Medium
CVE-2020-19188	gnu - ncurses	Buffer Overflow vulnerability in fmt_entry function in progs/dump_entry.c:1116 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	2023-08-22	6.5	Medium

CVE-2020-19189	gnu - ncurses	Buffer Overflow vulnerability in postprocess_terminfo function in tinfo/parse_entry.c:997 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	2023-08-22	6.5	Medium
CVE-2020-19190	gnu - ncurses	Buffer Overflow vulnerability in _nc_find_entry in tinfo/comp_hash.c:70 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	2023-08-22	6.5	Medium
CVE-2023-37435	arubanetworks - edgeconnect_sd-wan_orchestrator	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	6.5	Medium
CVE-2023-37436	arubanetworks - edgeconnect_sd-wan_orchestrator	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	6.5	Medium
CVE-2023-37437	arubanetworks - edgeconnect_sd-wan_orchestrator	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	6.5	Medium
CVE-2023-37438	arubanetworks - edgeconnect_sd-wan_orchestrator	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	6.5	Medium
CVE-2023-20169	cisco - nx-os	A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco NX-OS Software for the Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload. This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the unexpected restart of the IS-IS process, which could cause the affected device to reload. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2 adjacent to the affected device.	2023-08-23	6.5	Medium
CVE-2023-34972	qnap - multiple products	A cleartext transmission of sensitive information vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows local network clients to read the contents of unexpected sensitive data via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QuTS hero h5.1.0.2424 build 20230609 and later	2023-08-24	6.5	Medium
CVE-2023-3481	google - critters	Critters versions 0.0.17-0.0.19 have an issue when parsing the HTML, which leads to a potential cross-site scripting (XSS) bug. We recommend upgrading to version 0.0.20 of the extension.	2023-08-21	6.1	Medium
CVE-2023-4303	jenkins - fortify	Jenkins Fortify Plugin 22.1.38 and earlier does not escape the error message for a form validation method, resulting in an HTML injection vulnerability.	2023-08-21	6.1	Medium
CVE-2020-22181	samsung - sww-3400rw_firmware	A reflected cross site scripting (XSS) vulnerability was discovered on Samsung sww-3400rw Router devices via the m2 parameter of the sess-bin/command.cgi	2023-08-22	6.1	Medium

CVE-2020-23992	nagios - nagios_xi	Cross Site Scripting (XSS) in Nagios XI 5.7.1 allows remote attackers to run arbitrary code via returnUrl parameter in a crafted GET request.	2023-08-22	6.1	Medium
CVE-2022-41444	cacti - cacti	Cross Site Scripting (XSS) vulnerability in Cacti 1.2.21 via crafted POST request to graphs_new.php.	2023-08-22	6.1	Medium
CVE-2022-48547	cacti - cacti	A reflected cross-site scripting (XSS) vulnerability in Cacti 0.8.7g and earlier allows unauthenticated remote attackers to inject arbitrary web script or HTML in the "ref" parameter at auth_changepassword.php.	2023-08-22	6.1	Medium
CVE-2023-37425	arubanetworks - multiple products	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-08-22	6.1	Medium
CVE-2023-37439	arubanetworks - multiple products	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	2023-08-22	6.1	Medium
CVE-2023-32516	oracle - restaurant_menu_-_food_ordering_system_-_table_reservation	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in GloriaFood Restaurant Menu – Food Ordering System – Table Reservation plugin <= 2.3.6 versions.	2023-08-24	6.1	Medium
CVE-2023-41080	apache - multiple products	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92. The vulnerability is limited to the ROOT (default) web application.	2023-08-25	6.1	Medium
CVE-2023-39441	apache - multiple products	Apache Airflow SMTP Provider before 1.3.0, Apache Airflow IMAP Provider before 3.3.0, and Apache Airflow before 2.7.0 are affected by the Validation of OpenSSL Certificate vulnerability. The default SSL context with SSL library did not check a server's X.509 certificate. Instead, the code accepted any certificate, which could result in the disclosure of mail server credentials or mail contents when the client connects to an attacker in a MITM position. Users are strongly advised to upgrade to Apache Airflow version 2.7.0 or newer, Apache Airflow IMAP Provider version 3.3.0 or newer, and Apache Airflow SMTP Provider version 1.3.0 or newer to mitigate the risk associated with this vulnerability	2023-08-23	5.9	Medium
CVE-2023-4459	linux - linux_kernel	A NULL pointer dereference flaw was found in vmxnet3_rq_cleanup in drivers/net/vmxnet3/vmxnet3_drv.c in the networking sub-component in vmxnet3 in the Linux Kernel. This issue may allow a local attacker with normal user privilege to cause a denial of service due to a missing sanity check during cleanup.	2023-08-21	5.5	Medium
CVE-2020-19724	gnu - binutils	A memory consumption issue in get_data function in binutils/nm.c in GNU nm before 2.34 allows attackers to cause a denial of service via crafted command.	2023-08-22	5.5	Medium
CVE-2020-21490	gnu - binutils	An issue was discovered in GNU Binutils 2.34. It is a memory leak when process microblaze-dis.c. This one will consume memory on each insn disassembled.	2023-08-22	5.5	Medium
CVE-2022-35205	gnu - binutils	An issue was discovered in Binutils readelf 2.38.50, reachable assertion failure in function display_debug_names allows attackers to cause a denial of service.	2023-08-22	5.5	Medium
CVE-2022-35206	gnu - binutils	Null pointer dereference vulnerability in Binutils readelf 2.38.50 via function read_and_display_attr_value in file dwarf.c.	2023-08-22	5.5	Medium
CVE-2022-47007	gnu - binutils	An issue was discovered function stab_demangle_v3_arg in stabs.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	2023-08-22	5.5	Medium
CVE-2022-47008	gnu - binutils	An issue was discovered function make_tempdir, and make_tempname in bucomm.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	2023-08-22	5.5	Medium
CVE-2022-47010	gnu - binutils	An issue was discovered function pr_function_type in prdbg.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	2023-08-22	5.5	Medium

CVE-2022-47011	gnu - binutils	An issue was discovered function parse_stab_struct_fields in stabs.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	2023-08-22	5.5	Medium
CVE-2022-48063	gnu - binutils	GNU Binutils before 2.40 was discovered to contain an excessive memory consumption vulnerability via the function load_separate_debug_files at dwarf2.c. The attacker could supply a crafted ELF file and cause a DNS attack.	2023-08-22	5.5	Medium
CVE-2022-48064	gnu - binutils	GNU Binutils before 2.40 was discovered to contain an excessive memory consumption vulnerability via the function bfd_dwarf2_find_nearest_line_with_alt at dwarf2.c. The attacker could supply a crafted ELF file and cause a DNS attack.	2023-08-22	5.5	Medium
CVE-2022-48065	gnu - binutils	GNU Binutils before 2.40 was discovered to contain a memory leak vulnerability var the function find_abstract_instance in dwarf2.c.	2023-08-22	5.5	Medium
CVE-2023-40371	ibm - multiple products	IBM AIX 7.2, 7.3, VIOS 3.1's OpenSSH implementation could allow a non-privileged local user to access files outside of those allowed due to improper access controls. IBM X-Force ID: 263476.	2023-08-24	5.5	Medium
CVE-2023-39287	mitel - mivoice_connect	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 SP3 (22.24.5800.0) could allow an authenticated attacker with elevated privileges and internal network access to conduct a command argument injection due to insufficient parameter sanitization. A successful exploit could allow an attacker to access network information and to generate excessive network traffic.	2023-08-25	5.5	Medium
CVE-2023-39288	mitel - mivoice_connect	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect through 9.6.2304.102 could allow an authenticated attacker with elevated privileges and internal network access to conduct a command argument injection due to insufficient parameter sanitization. A successful exploit could allow an attacker to access network information and to generate excessive network traffic.	2023-08-25	5.5	Medium
CVE-2023-4301	jenkins - fortify	A cross-site request forgery (CSRF) vulnerability in Jenkins Fortify Plugin 22.1.38 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-08-21	5.4	Medium
CVE-2023-37421	arubanetworks - multiple products	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-08-22	5.4	Medium
CVE-2023-37422	arubanetworks - multiple products	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-08-22	5.4	Medium
CVE-2023-37423	arubanetworks - multiple products	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-08-22	5.4	Medium
CVE-2023-20115	cisco - multiple products	A vulnerability in the SFTP server implementation for Cisco Nexus 3000 Series Switches and 9000 Series Switches in standalone NX-OS mode could allow an authenticated, remote attacker to download or overwrite files from the underlying operating system of an affected device. This vulnerability is due to a logic error when verifying the user role when an SFTP connection is opened to an affected device. An attacker could exploit this vulnerability by connecting and authenticating via SFTP as a valid, non-administrator user. A successful exploit could allow the attacker to read or overwrite files from the underlying operating system with the privileges of the authenticated user. There are workarounds that address this vulnerability.	2023-08-23	5.4	Medium
CVE-2023-20230	cisco - multiple products	A vulnerability in the restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to read, modify, or delete non-tenant policies (for example, access policies) created by users associated with a different security domain on an affected system.	2023-08-23	5.4	Medium

		This vulnerability is due to improper access control when restricted security domains are used to implement multi-tenancy for policies outside the tenant boundaries. An attacker with a valid user account associated with a restricted security domain could exploit this vulnerability. A successful exploit could allow the attacker to read, modify, or delete policies created by users associated with a different security domain. Exploitation is not possible for policies under tenants that an attacker has no authorization to access.			
CVE-2022-48538	cacti - cacti	In Cacti 1.2.19, there is an authentication bypass in the web login functionality because of improper validation in the PHP code: cacti_ldap_auth() allows a zero as the password.	2023-08-22	5.3	Medium
CVE-2023-37440	arubanetworks - edgeconnect_sd-wan_orchestrator	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an unauthenticated remote attacker to conduct a server-side request forgery (SSRF) attack. A successful exploit allows an attacker to enumerate information about the internal structure of the EdgeConnect SD-WAN Orchestrator host leading to potential disclosure of sensitive information.	2023-08-22	5.3	Medium
CVE-2023-40370	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7.1 runtime is vulnerable to information disclosure of script content if the remote REST request computer policy is enabled. IBM X-Force ID: 263470.	2023-08-22	5.3	Medium
CVE-2023-34973	qnap - multiple products	An insufficient entropy vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows remote users to predict secret via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QuTS hero h5.1.0.2424 build 20230609 and later	2023-08-24	5.3	Medium
CVE-2023-39290	mitel - mivoice_connect	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through R19.3 SP3 (22.24.5800.0) could allow an authenticated attacker with elevated privileges to conduct an information disclosure attack due to improper configuration. A successful exploit could allow an attacker to view system information.	2023-08-25	4.9	Medium
CVE-2023-39291	mitel - mivoice_connect	A vulnerability in the Connect Mobility Router component of MiVoice Connect through 9.6.2304.102 could allow an authenticated attacker with elevated privileges to conduct an information disclosure attack due to improper configuration. A successful exploit could allow an attacker to view system information.	2023-08-25	4.9	Medium
CVE-2022-44730	apache - xml_graphics_batik	Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache XML Graphics Batik.This issue affects Apache XML Graphics Batik: 1.16. A malicious SVG can probe user profile / data and send it directly as parameter to a URL.	2023-08-22	4.4	Medium
CVE-2022-3743	lenovo - ideapad_1_14iau7_firmware	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges under certain conditions the ability to enumerate Embedded Controller (EC) commands.	2023-08-23	4.4	Medium
CVE-2022-3745	lenovo - ideapad_1_14iau7_firmware	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to view incoming and returned data from SMI.	2023-08-23	4.4	Medium
CVE-2023-4302	jenkins - fortify	A missing permission check in Jenkins Fortify Plugin 22.1.38 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-08-21	4.3	Medium
CVE-2023-38732	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7 server could allow an authenticated user to view sensitive information from application logs. IBM X-Force ID: 262289.	2023-08-22	4.3	Medium
CVE-2023-38733	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7.1 and 23.0.0 through 23.0.1 server could allow an authenticated user to view sensitive information from installation logs. IBM X-Force Id: 262293.	2023-08-22	4.3	Medium
CVE-2023-38158	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-08-21	3.1	Low

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.