الهيئة الوطنية للأمن السيبراني
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 4th of February to 10th of February. 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 ٤ فبراير إلى ١٠ فبراير. 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-2024-20011	google - multiple products	In alac decoder, there is a possible information disclosure due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08441146; Issue ID: ALPS08441146.	2024-02-05	9.8	Critical
CVE-2024-23108	fortinet - multiple products	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.1.0 through 7.1.1 and 7.0.0 through 7.0.2 and 6.7.0 through 6.7.8 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.2 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via via crafted API requests.	2024-02-05	9.8	Critical
CVE-2024-23109	fortinet - multiple products	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.1.0 through 7.1.1 and 7.0.0 through 7.0.2 and 6.7.0 through 6.7.8 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.2 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via via crafted API requests.	2024-02-05	9.8	Critical
CVE-2023-43518	qualcomm - aqt1000_firmware	Memory corruption in video while parsing invalid mp2 clip.	2024-02-06	9.8	Critical
CVE-2023-43519	qualcomm - aqt1000_firmware	Memory corruption in video while parsing the Videoinfo, when the size of atom is greater than the videoinfo size.	2024-02-06	9.8	Critical
CVE-2023-43520	qualcomm - ar8035_firmware	Memory corruption when AP includes TID to link mapping IE in the beacons and STA is parsing the beacon TID to link mapping IE.	2024-02-06	9.8	Critical
CVE-2023-43534	qualcomm - ar8035_firmware	Memory corruption while validating the TID to Link Mapping action request frame, when a station connects to an access point.	2024-02-06	9.8	Critical
CVE-2024-22433	dell - data_protection_search	Dell Data Protection Search 19.2.0 and above contain an exposed password opportunity in plain text when using LdapSettings.get_ldap_info in DP Search. A remote unauthorized unauthenticated attacker could potentially exploit this vulnerability leading to a loss of Confidentiality, Integrity, Protection, and remote takeover of the system. This is a high-severity vulnerability as it allows an attacker to take complete control of DP Search to affect downstream protected devices.	2024-02-06	9.8	Critical
CVE-2024-1283	google - chrome	Heap buffer overflow in Skia in Google Chrome prior to 121.0.6167.160 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-02-07	9.8	Critical
CVE-2024-1284	google - chrome	Use after free in Mojo in Google Chrome prior to 121.0.6167.160 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-02-07	9.8	Critical
CVE-2023-32328	ibm - security_verify_access	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 uses insecure protocols in some instances that could allow an attacker on the network to take control of the server. IBM X-Force Id: 254957.	2024-02-07	9.8	Critical
CVE-2023-32330	ibm - security_verify_access	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 uses insecure calls that could allow an attacker on the network to take control of the server. IBM X-Force ID: 254977.	2024-02-07	9.8	Critical

CVE-2024-22394	sonicwall - sonicos	An improper authentication vulnerability has been identified in SonicWall SonicOS SSL-VPN feature, which in specific conditions could allow a remote attacker to bypass authentication. This issue affects only firmware version SonicOS 7.1.1-7040.	2024-02-08	9.8	Critical
CVE-2023-40266	mitel - unify_openscape_xpressions_webassistant	An issue was discovered in Atos Unify OpenScape Xpressions WebAssistant V7 before V7R1 FR5 HF42 P911. It allows path traversal.	2024-02-08	9.8	Critical
CVE-2024-21762	fortinet - multiple products	A out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests	2024-02-09	9.8	Critical
CVE-2023-33058	qualcomm - ar8035_firmware	Information disclosure in Modem while processing SIB5.	2024-02-06	9.1	Critical
CVE-2024-20009	google - multiple products	In alac decoder, there is a possible out of bounds write due to an incorrect error handling. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08441150; Issue ID: ALPS08441150.	2024-02-05	8.8	High
CVE-2023-7216	gnu - cpio	A path traversal vulnerability was found in the CPIO utility. This issue could allow a remote unauthenticated attacker to trick a user into opening a specially crafted archive. During the extraction process, the archiver could follow symlinks outside of the intended directory, which could be utilized to run arbitrary commands on the target system.	2024-02-05	8.8	High
CVE-2023-35188	solarwinds - solarwinds_platform	SQL Injection Remote Code Execution Vulnerability was found using a create statement in the SolarWinds Platform. This vulnerability requires user authentication to be exploited.	2024-02-06	8.8	High
CVE-2023-50395	solarwinds - solarwinds_platform	SQL Injection Remote Code Execution Vulnerability was found using an update statement in the SolarWinds Platform. This vulnerability requires user authentication to be exploited	2024-02-06	8.8	High
CVE-2024-22022	veeam - recovery_orchestrator	Vulnerability CVE-2024-22022 allows a Veeam Recovery Orchestrator user that has been assigned a low-privileged role to access the NTLM hash of the service account used by the Veeam Orchestrator Server Service.	2024-02-07	8.8	High
CVE-2024-20252	cisco - expressway	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks that perform arbitrary actions on an affected device. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory.	2024-02-07	8.8	High
CVE-2024-20254	cisco - expressway	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks that perform arbitrary actions on an affected device. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory.	2024-02-07	8.8	High
CVE-2023-40265	mitel - unify_openscape_xpressions_webassistant	An issue was discovered in Atos Unify OpenScape Xpressions WebAssistant V7 before V7R1 FR5 HF42 P911. It allows authenticated remote code execution via file upload.	2024-02-08	8.8	High
CVE-2023-45187	ibm - multiple products	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 268749.	2024-02-09	8.8	High
CVE-2023-50386	apache - multiple products	Improper Control of Dynamically-Managed Code Resources, Unrestricted Upload of File with Dangerous Type, Inclusion of	2024-02-09	8.8	High

		Functionality from Untrusted Control Sphere vulnerability in Apache Solr.This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. In the affected versions, Solr ConfigSets accepted Java jar and class files to be uploaded through the ConfigSets API. When backing up Solr Collections, these configSet files would be saved to disk when using the LocalFileSystemRepository (the default for backups). If the backup was saved to a directory that Solr uses in its ClassPath/ClassLoaders, then the jar and class files would be available to use with any ConfigSet, trusted or untrusted. When Solr is run in a secure way (Authorization enabled), as is strongly suggested, this vulnerability is limited to extending the Backup permissions with the ability to add libraries. Users are recommended to upgrade to version 8.11.3 or 9.4.1, which fix the issue. In these versions, the following protections have been added: * Users are no longer able to upload files to a configSet that could be executed via a Java ClassLoader. * The Backup API restricts saving backups to directories that are used in the ClassLoader.			
CVE-2024-25148	liferay - multiple products	In Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions the `doAsUserId` URL parameter may get leaked when creating linked content using the WYSIWYG editor and while impersonating a user. This may allow remote authenticated users to impersonate a user after accessing the linked content.	2024-02-08	8.1	High
CVE-2024-20015	google - multiple products	In telephony, there is a possible escalation of privilege due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08441419; Issue ID: ALPS08441419.	2024-02-05	7.8	High
CVE-2024-20812	samsung - multiple products	Out-of-bounds Write in padmd_vld_htbl of libpadm.so prior to SMR Feb-2024 Release 1 allows local attacker to execute arbitrary code.	2024-02-06	7.8	High
CVE-2024-20813	samsung - multiple products	Out-of-bounds Write in padmd_vld_qtbl of libpadm.so prior to SMR Feb-2024 Release 1 allows local attacker to execute arbitrary code.	2024-02-06	7.8	High
CVE-2024-20817	samsung - multiple products	Out out bounds Write vulnerabilities in svc1td_vld_slh of libsthmbc.so prior to SMR Feb-2024 Release 1 allows local attackers to trigger buffer overflow.	2024-02-06	7.8	High
CVE-2024-20818	samsung - multiple products	Out out bounds Write vulnerabilities in svc1td_vld_elh of libsthmbc.so prior to SMR Feb-2024 Release 1 allows local attackers to trigger buffer overflow.	2024-02-06	7.8	High
CVE-2024-20819	samsung - multiple products	Out out bounds Write vulnerabilities in svc1td_vld_plh_ap of libsthmbc.so prior to SMR Feb-2024 Release 1 allows local attackers to trigger buffer overflow.	2024-02-06	7.8	High
CVE-2023-33067	qualcomm - 9206_lte_modem_firmware	Memory corruption in Audio while calling START command on host voice PCM multiple times for the same RX or TX tap points.	2024-02-06	7.8	High
CVE-2023-33068	qualcomm - 9206_lte_modem_firmware	Memory corruption in Audio while processing IIR config data from AFE calibration block.	2024-02-06	7.8	High
CVE-2023-33069	qualcomm - 9206_lte_modem_firmware	Memory corruption in Audio while processing the calibration data returned from ACDB loader.	2024-02-06	7.8	High
CVE-2023-33072	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Core while processing control functions.	2024-02-06	7.8	High
CVE-2023-33076	qualcomm - aqt1000_firmware	Memory corruption in Core when updating rollback version for TA and OTA feature is enabled.	2024-02-06	7.8	High
CVE-2023-33077	qualcomm - aqt1000_firmware	Memory corruption in HLOS while converting from authorization token to HIDL vector.	2024-02-06	7.8	High
CVE-2023-43513	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while processing the event ring, the context read pointer is untrusted to HLOS and when it is passed with arbitrary values, may point to address in the middle of ring element.	2024-02-06	7.8	High
CVE-2023-43516	qualcomm - fastconnect_6900_firmware	Memory corruption when malformed message payload is received from firmware.	2024-02-06	7.8	High
CVE-2023-43517	qualcomm - qam8255p_firmware	Memory corruption in Automotive Multimedia due to improper access control in HAB.	2024-02-06	7.8	High

CVE-2023-43532	qualcomm - fastconnect_6700_firmware	Memory corruption while reading ACPI config through the user mode app.	2024-02-06	7.8	High
CVE-2023-43535	qualcomm - fastconnect_6700_firmware	Memory corruption when negative display IDs are sent as input while processing DISPLAYESCAPE event trigger.	2024-02-06	7.8	High
CVE-2023-25543	dell - power_manager	Dell Power Manager, versions prior to 3.14, contain an Improper Authorization vulnerability in DPM service. A low privileged malicious user could potentially exploit this vulnerability in order to elevate privileges on the system.	2024-02-06	7.8	High
CVE-2023-32451	dell - display_manager	Dell Display Manager application, version 2.1.1.17, contains a vulnerability that low privilege user can execute malicious code during installation and uninstallation	2024-02-06	7.8	High
CVE-2023-32479	dell - multiple products	Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management Server versions prior to 11.9.0 contain privilege escalation vulnerability due to improper ACL of the non-default installation directory. A local malicious user could potentially exploit this vulnerability by replacing binaries in installed directory and taking reverse shell of the system leading to Privilege Escalation.	2024-02-06	7.8	High
CVE-2024-22237	vmware - aria_operations_for_networks	Aria Operations for Networks contains a local privilege escalation vulnerability. A console user with access to Aria Operations for Networks may exploit this vulnerability to escalate privileges to gain root access to the system.	2024-02-06	7.8	High
CVE-2024-22239	vmware - aria_operations_for_networks	Aria Operations for Networks contains a local privilege escalation vulnerability. A console user with access to Aria Operations for Networks may exploit this vulnerability to escalate privileges to gain regular shell access.	2024-02-06	7.8	High
CVE-2024-22012	google - android	In TBD of TBD, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-02-07	7.8	High
CVE-2024-22313	ibm - storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 278749.	2024-02-10	7.8	High
CVE-2024-20007	google - multiple products	In mp3 decoder, there is a possible out of bounds write due to a race condition. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08441369; Issue ID: ALPS08441369.	2024-02-05	7.5	High
CVE-2023-27318	netapp - storagegrid	StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.13 are susceptible to a Denial of Service (DoS) vulnerability. A successful exploit could lead to a crash of the Local Distribution Router (LDR) service.	2024-02-05	7.5	High
CVE-2023-50781	redhat - multiple products	A flaw was found in m2crypto. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data.	2024-02-05	7.5	High
CVE-2023-50782	redhat - ansible_automation_platform	A flaw was found in the python-cryptography package. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data.	2024-02-05	7.5	High
CVE-2023-33049	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in Multi-Mode Call Processor due to UE failure because of heap leakage.	2024-02-06	7.5	High
CVE-2023-33057	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in Multi-Mode Call Processor while processing UE policy container.	2024-02-06	7.5	High
CVE-2023-43522	qualcomm - aqt1000_firmware	Transient DOS while key unwrapping process, when the given encrypted key is empty or NULL.	2024-02-06	7.5	High
CVE-2023-43523	qualcomm - ar8035_firmware	Transient DOS while processing 11AZ RTT management action frame received through OTA.	2024-02-06	7.5	High
CVE-2023-43533	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in WLAN Firmware when the length of received beacon is less than length of ieee802.11 beacon frame.	2024-02-06	7.5	High
CVE-2023-43536	qualcomm - 315_5g_iot_modem_firmware	Transient DOS while parse fils IE with length equal to 1.	2024-02-06	7.5	High
CVE-2023-4503	redhat - multiple products	An improper initialization vulnerability was found in Galleon. When using Galleon to provision custom EAP or EAP-XP servers, the servers are created unsecured. This issue could allow an attacker to access remote HTTP services available from the server.	2024-02-06	7.5	High

CVE-2024-23673	apache - sling_servlets_resolver	Malicious code execution via path traversal in Apache Software Foundation Apache Sling Servlets Resolver.This issue affects all version of Apache Sling Servlets Resolver before 2.11.0. However, whether a system is vulnerable to this attack depends on the exact configuration of the system. If the system is vulnerable, a user with write access to the repository might be able to trick the Sling Servlet Resolver to load a previously uploaded script. Users are recommended to upgrade to version 2.11.0, which fixes this issue. It is recommended to upgrade, regardless of whether your system configuration currently allows this attack or not.	2024-02-06	7.5	High
CVE-2023-38369	ibm - security_access_manager_container	IBM Security Access Manager Container 10.0.0.0 through 10.0.6.1 does not require that docker images should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 261196.	2024-02-07	7.5	High
CVE-2023-47700	ibm - storage_virtualize	IBM SAN Volume Controller, IBM Storwize, IBM FlashSystem and IBM Storage Virtualize 8.6 products could allow a remote attacker to spoof a trusted system that would not be correctly validated by the Storwize server. This could lead to a user connecting to a malicious host, believing that it was a trusted system and deceived into accepting spoofed data. IBM X-Force ID: 271016.	2024-02-07	7.5	High
CVE-2024-20290	cisco - multiple products	A vulnerability in the OLE2 file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an incorrect check for end-of-string values during scanning, which may result in a heap buffer over-read. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software and consuming available system resources. For a description of this vulnerability, see the ClamAV blog .	2024-02-07	7.5	High
CVE-2023-6356	linux - linux_kernel	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver and causing kernel panic and a denial of service.	2024-02-07	7.5	High
CVE-2023-6535	linux - linux_kernel	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kernel panic and a denial of service.	2024-02-07	7.5	High
CVE-2023-6536	linux - linux_kernel	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kernel panic and a denial of service.	2024-02-07	7.5	High
CVE-2024-23452	apache - brpc	Request smuggling vulnerability in HTTP server in Apache bRPC 0.9.5~1.7.0 on all platforms allows attacker to smuggle request. Vulnerability Cause Description? The http_parser does not comply with the RFC-7230 HTTP 1.1 specification. Attack scenario: If a message is received with both a Transfer-Encoding and a Content-Length header field, such a message might indicate an attempt to perform request smuggling or response splitting. One particular attack scenario is that a bRPC made http server on the backend receiving requests in one persistent connection from frontend server that uses TE to parse request with the logic that 'chunk' is contained in the TE field. in that case an attacker can smuggle a request into the connection to the backend server. Solution: You can choose one solution from below: 1. Upgrade bRPC to version 1.8.0, which fixes this issue. Download link: https://github.com/apache/brpc/releases/tag/1.8.0 2. Apply this patch: https://github.com/apache/brpc/pull/2518	2024-02-08	7.5	High
CVE-2023-45191	ibm - multiple products	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 uses an inadequate account lockout setting that could allow a remote	2024-02-09	7.5	High

		attacker to brute force account credentials. IBM X-Force ID: 268755.			
CVE-2023-50291	apache - multiple products	Insufficiently Protected Credentials vulnerability in Apache Solr. This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.3.0. One of the two endpoints that publishes the Solr process' Java system properties, /admin/info/properties, was only setup to hide system properties that had "password" contained in the name. There are a number of sensitive system properties, such as "basicauth" and "aws.secretKey" do not contain "password", thus their values were published via the "/admin/info/properties" endpoint. This endpoint populates the list of System Properties on the home screen of the Solr Admin page, making the exposed credentials visible in the UI. This /admin/info/properties endpoint is protected under the "config-read" permission. Therefore, Solr Clouds with Authorization enabled will only be vulnerable through logged-in users that have the "config-read" permission. Users are recommended to upgrade to version 9.3.0 or 8.11.3, which fixes the issue. A single option now controls hiding Java system property for all endpoints, "-Dsolr.hiddenSysProps". By default all known sensitive properties are hidden (including "-Dbasicauth"), as well as any property with a name containing "secret" or "password". Users who cannot upgrade can also use the following Java system property to fix the issue: '-Dsolr.redaction.system.pattern=.*(password|secret|basicauth).*'	2024-02-09	7.5	High
CVE-2023-50292	apache - multiple products	Incorrect Permission Assignment for Critical Resource, Improper Control of Dynamically-Managed Code Resources vulnerability in Apache Solr. This issue affects Apache Solr: from 8.10.0 through 8.11.2, from 9.0.0 before 9.3.0. The Schema Designer was introduced to allow users to more easily configure and test new Schemas and configSets. However, when the feature was created, the "trust" (authentication) of these configSets was not considered. External library loading is only available to configSets that are "trusted" (created by authenticated users), thus non-authenticated users are unable to perform Remote Code Execution. Since the Schema Designer loaded configSets without taking their "trust" into account, configSets that were created by unauthenticated users were allowed to load external libraries when used in the Schema Designer. Users are recommended to upgrade to version 9.3.0, which fixes the issue.	2024-02-09	7.5	High
CVE-2023-50298	apache - multiple products	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Solr.This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. Solr Streaming Expressions allows users to extract data from other Solr Clouds, using a "zkHost" parameter. When original SolrCloud is setup to use ZooKeeper credentials and ACLs, they will be sent to whatever "zkHost" the user provides. An attacker could setup a server to mock ZooKeeper, that accepts ZooKeeper requests with credentials and ACLs and extracts the sensitive information, then send a streaming expression using the mock server's address in "zkHost". Streaming Expressions are exposed via the "/streaming" handler, with "read" permissions. Users are recommended to upgrade to version 8.11.3 or 9.4.1, which fix the issue. From these versions on, only zkHost values that have the same server address (regardless of chroot), will use the given ZooKeeper credentials and ACLs when connecting.	2024-02-09	7.5	High
CVE-2024-22361	ibm - multiple products	IBM Semeru Runtime 8.0.302.0 through 8.0.392.0, 11.0.12.0 through 11.0.21.0, 17.0.1.0 - 17.0.9.0, and 21.0.1.0 uses weaker than expected cryptographic algorithms that could allow an	2024-02-10	7.5	High

		attacker to decrypt highly sensitive information. IBM X-Force ID: 281222.			
CVE-2023-51437	apache - multiple products	Observable timing discrepancy vulnerability in Apache Pulsar SASL Authentication Provider can allow an attacker to forge a SASL Role Token that will pass signature verification. Users are recommended to upgrade to version 2.11.3, 3.0.2, or 3.1.1 which fixes the issue. Users should also consider updating the configured secret in the `saslJaasServerRoleTokenSignerSecretPath` file. Any component matching an above version running the SASL Authentication Provider is affected. That includes the Pulsar Broker, Proxy, Websocket Proxy, or Function Worker. 2.11 Pulsar users should upgrade to at least 2.11.3. 3.0 Pulsar users should upgrade to at least 3.0.2. 3.1 Pulsar users should upgrade to at least 3.1.1. Any users running Pulsar 2.8, 2.9, 2.10, and earlier should upgrade to one of the above patched versions. For additional details on this attack vector, please refer to https://codahale.com/a-lesson-in-timing-attacks/ .	2024-02-07	7.4	High
CVE-2023-36498	tp-link - er7206_firmware	A post-authentication command injection vulnerability exists in the PPTP client functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability and gain access to an unrestricted shell.	2024-02-06	7.2	High
CVE-2023-42664	tp-link - er7206_firmware	A post authentication command injection vulnerability exists when setting up the PPTP global configuration of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-43482	tp-link - er7206_firmware	A command execution vulnerability exists in the guest resource functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-46683	tp-link - er7206_firmware	A post authentication command injection vulnerability exists when configuring the wireguard VPN functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection . An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-47167	tp-link - er7206_firmware	A post authentication command injection vulnerability exists in the GRE policy functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-47209	tp-link - er7206_firmware	A post authentication command injection vulnerability exists in the ipsec policy functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-47617	tp-link - er7206_firmware	A post authentication command injection vulnerability exists when configuring the web group member of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-47618	tp-link - er7206_firmware	A post authentication command execution vulnerability exists in the web filtering functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	High
CVE-2023-43017	ibm - security_verify_access	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 could allow a privileged user to install a configuration file that could allow remote access. IBM X-Force ID: 266155.	2024-02-07	7.2	High
CVE-2023-50957	ibm - storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 could allow a privileged user to perform unauthorized actions after obtaining encrypted data from clear text key storage. IBM X-Force ID: 275783.	2024-02-10	7.2	High
CVE-2024-20820	samsung - multiple products	Improper input validation in bootloader prior to SMR Feb-2024 Release 1 allows attacker to cause an Out-Of-Bounds read.	2024-02-06	7.1	High
CVE-2023-33065	qualcomm - aqt1000_firmware	Information disclosure in Audio while accessing AVCS services from ADSP payload.	2024-02-06	7.1	High

CVE-2023-28049	dell - command_|_monitor	Dell Command | Monitor, versions prior to 10.9, contain an arbitrary folder deletion vulnerability. A locally authenticated malicious user may exploit this vulnerability in order to perform a privileged arbitrary file delete.	2024-02-06	7.1	High
CVE-2023-32454	dell - update_package_framework	DUP framework version 4.9.4.36 and prior contains insecure operation on Windows junction/Mount point vulnerability. A local malicious standard user could exploit the vulnerability to create arbitrary files, leading to denial of service	2024-02-06	7.1	High
CVE-2024-20255	cisco - expressway	A vulnerability in the SOAP API of Cisco Expressway Series and Cisco TelePresence Video Communication Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected system. An attacker could exploit this vulnerability by persuading a user of the REST API to follow a crafted link. A successful exploit could allow the attacker to cause the affected system to reload.	2024-02-07	7.1	High
CVE-2023-33046	qualcomm - ar8035_firmware	Memory corruption in Trusted Execution Environment while deinitializing an object used for license validation.	2024-02-06	7	High
CVE-2024-24857	linux - multiple products	A race condition was found in the Linux kernel's net/bluetooth device driver in conn_info_{min,max}_age_set() function. This can result in integrity overflow issue, possibly leading to bluetooth connection abnormality or denial of service.	2024-02-05	6.8	Medium
CVE-2024-22464	dell - emc_appsync	Dell EMC AppSync, versions from 4.2.0.0 to 4.6.0.0 including all Service Pack releases, contain an exposure of sensitive information vulnerability in AppSync server logs. A high privileged remote attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable system with privileges of the compromised account.	2024-02-08	6.8	Medium
CVE-2024-20001	google - multiple products	In TVAPI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03961601; Issue ID: DTV03961601.	2024-02-05	6.7	Medium
CVE-2024-20002	google - multiple products	In TVAPI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03961715; Issue ID: DTV03961715.	2024-02-05	6.7	Medium
CVE-2024-20010	google - multiple products	In keyInstall, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08358560; Issue ID: ALPS08358560.	2024-02-05	6.7	Medium
CVE-2024-20012	google - multiple products	In keyInstall, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08358566; Issue ID: ALPS08358566.	2024-02-05	6.7	Medium
CVE-2024-20013	google - multiple products	In keyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08471742; Issue ID: ALPS08308608.	2024-02-05	6.7	Medium
CVE-2023-32474	dell - display_manager	Dell Display Manager application, version 2.1.1.17 and prior, contain an insecure operation on windows junction/mount point. A local malicious user could potentially exploit this vulnerability during installation leading to arbitrary folder or file deletion	2024-02-06	6.6	Medium
CVE-2023-6240	linux - linux_kernel	A Marvin vulnerability side-channel leakage was found in the RSA decryption operation in the Linux Kernel. This issue may allow a network attacker to decrypt ciphertexts or forge signatures, limiting the services that use that private key.	2024-02-04	6.5	Medium
CVE-2024-20815	samsung - multiple products	Improper authentication vulnerability in onCharacteristicReadRequest in Auto Hotspot prior to SMR Feb-2024 Release 1 allows adjacent attackers connect to victim&#39;s mobile hotspot without user awareness.	2024-02-06	6.5	Medium
CVE-2024-20816	samsung - multiple products	Improper authentication vulnerability in onCharacteristicWriteRequest in Auto Hotspot prior to SMR Feb-	2024-02-06	6.5	Medium

		2024 Release 1 allows adjacent attackers connect to victim&#39;s mobile hotspot without user awareness.				
CVE-2024-25144	liferay - multiple products	The IFrame widget in Liferay Portal 7.2.0 through 7.4.3.26, and older unsupported versions, and Liferay DXP 7.4 before update 27, 7.3 before update 6, 7.2 before fix pack 19, and older unsupported versions does not check the URL of the IFrame, which allows remote authenticated users to cause a denial-of-service (DoS) via a self referencing IFrame.	2024-02-08	6.5	Medium
CVE-2023-32341	ibm - multiple products	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 could allow an authenticated user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 255827.	2024-02-09	6.5	Medium
CVE-2024-22332	ibm - integration_bus	The IBM Integration Bus for z/OS 10.1 through 10.1.0.2 AdminAPI is vulnerable to a denial of service due to file system exhaustion. IBM X-Force ID: 279972.	2024-02-09	6.5	Medium
CVE-2024-24861	linux - multiple products	A race condition was found in the Linux kernel's media/xc4000 device driver in xc4000 xc4000_get_frequency() function. This can result in return value overflow issue, possibly leading to malfunction or denial of service issue.	2024-02-05	6.3	Medium
CVE-2024-0953	mozilla - firefox	When a user scans a QR Code with the QR Code Scanner feature, the user is not prompted before being navigated to the page specified in the code. This may surprise the user and potentially direct them to unwanted content.	2024-02-05	6.1	Medium
CVE-2023-45190	ibm - multiple products	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 268754.	2024-02-09	6.1	Medium
CVE-2023-34042	vmware - multiple products	The spring-security.xsd file inside the spring-security-config jar is world writable which means that if it were extracted it could be written by anyone with access to the file system. While there are no known exploits, this is an example of “CWE-732: Incorrect Permission Assignment for Critical Resource” and could result in an exploit. Users should update to the latest version of Spring Security to mitigate any future exploits found around this issue.	2024-02-05	5.5	Medium
CVE-2024-20814	samsung - multiple products	Out-of-bounds Read in padmd_vld_ac_prog_refine of libpadm.so prior to SMR Feb-2024 Release 1 allows attacker access unauthorized information.	2024-02-06	5.5	Medium
CVE-2024-20822	samsung - galaxy_store	Implicit intent hijacking vulnerability in AccountActivity of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	Medium
CVE-2024-20823	samsung - galaxy_store	Implicit intent hijacking vulnerability in SamsungAccount of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	Medium
CVE-2024-20824	samsung - galaxy_store	Implicit intent hijacking vulnerability in VoiceSearch of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	Medium
CVE-2024-20825	samsung - galaxy_store	Implicit intent hijacking vulnerability in IAP of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	Medium
CVE-2024-20826	samsung - uphelper_library	Implicit intent hijacking vulnerability in UPHelper library prior to version 4.0.0 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	Medium
CVE-2023-33060	qualcomm - ar8035_firmware	Transient DOS in Core when DDR memory check is called while DDR is not initialized.	2024-02-06	5.5	Medium
CVE-2023-33064	qualcomm - aqt1000_firmware	Transient DOS in Audio when invoking callback function of ASM driver.	2024-02-06	5.5	Medium
CVE-2024-0684	gnu - multiple products	A flaw was found in the GNU coreutils "split" program. A heap overflow with user-controlled data of multiple hundred bytes in length could occur in the line_bytes_split() function, potentially leading to an application crash and denial of service.	2024-02-06	5.5	Medium
CVE-2024-0690	redhat - multiple products	An information disclosure flaw was found in ansible-core due to a failure to respect the ANSIBLE_NO_LOG configuration in some scenarios. It was discovered that information is still included in the output in certain tasks, such as loop items. Depending on the task,	2024-02-06	5.5	Medium

		this issue may include sensitive information, such as decrypted secret values.			
CVE-2024-0911	gnu - indent	A flaw was found in indent, a program for formatting C code. This issue may allow an attacker to trick a user into processing a specially crafted file to trigger a heap-based buffer overflow, causing the application to crash.	2024-02-06	5.5	Medium
CVE-2024-22331	ibm - multiple products	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.19, 7.1 through 7.1.2.15, 7.2 through 7.2.3.8, 7.3 through 7.3.2.3, and IBM UrbanCode Deploy (UCD) - IBM DevOps Deploy 8.0.0.0 could disclose sensitive user information when installing the Windows agent. IBM X-Force ID: 279971.	2024-02-06	5.5	Medium
CVE-2023-31002	ibm - security_access_manager_container	IBM Security Access Manager Container 10.0.0.0 through 10.0.6.1 temporarily stores sensitive information in files that could be accessed by a local user. IBM X-Force ID: 254657.	2024-02-07	5.5	Medium
CVE-2024-23769	samsung - magician	Improper privilege control for the named pipe in Samsung Magician PC Software 8.0.0 (for Windows) allows a local attacker to read privileged data.	2024-02-07	5.5	Medium
CVE-2024-22318	ibm - multiple products	IBM i Access Client Solutions (ACS) 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.4 is vulnerable to NT LAN Manager (NTLM) hash disclosure by an attacker modifying UNC capable paths within ACS configuration files to point to a hostile server. If NTLM is enabled, the Windows operating system will try to authenticate using the current user's session. The hostile server could capture the NTLM hash information to obtain the user's credentials. IBM X-Force ID: 279091.	2024-02-09	5.5	Medium
CVE-2024-22312	ibm - storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 278748.	2024-02-10	5.5	Medium
CVE-2023-50947	ibm - multiple products	IBM Business Automation Workflow 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 275665.	2024-02-04	5.4	Medium
CVE-2024-25145	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in the Portal Search module's Search Result app in Liferay Portal 7.2.0 through 7.4.3.11, and older unsupported versions, and Liferay DXP 7.4 before update 8, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML into the Search Result app's search result if highlighting is disabled by adding any searchable content (e.g., blog, message board message, web content article) to the application.	2024-02-07	5.4	Medium
CVE-2024-22119	zabbix - multiple products	The cause of vulnerability is improper validation of form input field “Name” on Graph page in Items section.	2024-02-09	5.4	Medium
CVE-2024-24858	linux - multiple products	A race condition was found in the Linux kernel's net/bluetooth in {conn,adv}_{min,max}_interval_set() function. This can result in I2cap connection or broadcast abnormality issue, possibly leading to denial of service.	2024-02-05	5.3	Medium
CVE-2024-24860	linux - multiple products	A race condition was found in the Linux kernel's bluetooth device driver in {min,max}_key_size_set() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	5.3	Medium
CVE-2023-39196	apache - ozone	Improper Authentication vulnerability in Apache Ozone. The vulnerability allows an attacker to download metadata internal to the Storage Container Manager service without proper authentication. The attacker is not allowed to do any modification within the Ozone Storage Container Manager service using this vulnerability. The accessible metadata does not contain sensitive information that can be used to exploit the system later on, and the accessible data does not make it possible to gain access to actual user data within Ozone. This issue affects Apache Ozone: 1.2.0 and subsequent releases up until 1.3.0. Users are recommended to upgrade to version 1.4.0, which fixes the issue.	2024-02-07	5.3	Medium
CVE-2024-25146	liferay - multiple products	Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 18, and older unsupported versions returns with different responses depending on whether a site does not exist or if the user does not have permission to access the site, which allows remote attackers	2024-02-08	5.3	Medium

		to discover the existence of sites by enumerating URLs. This vulnerability occurs if locale.prepend.friendly.url.style=2 and if a custom 404 page is used.			
CVE-2023-33851	ibm - multiple products	IBM PowerVM Hypervisor FW950.00 through FW950.90, FW1020.00 through FW1020.40, and FW1030.00 through FW1030.30 could reveal sensitive partition data to a system administrator. IBM X-Force ID: 257135.	2024-02-04	4.9	Medium
CVE-2024-22240	vmware - aria_operations_for_networks	Aria Operations for Networks contains a local file read vulnerability. A malicious actor with admin privileges may exploit this vulnerability leading to unauthorized access to sensitive information.	2024-02-06	4.9	Medium
CVE-2024-24859	linux - multiple products	A race condition was found in the Linux kernel's net/bluetooth in sniff_{min,max}_interval_set() function. This can result in a bluetooth sniffing exception issue, possibly leading denial of service.	2024-02-05	4.8	Medium
CVE-2024-22238	vmware - aria_operations_for_networks	Aria Operations for Networks contains a cross site scripting vulnerability. A malicious actor with admin privileges may be able to inject malicious code into user profile configurations due to improper input sanitization.	2024-02-06	4.8	Medium
CVE-2024-22241	vmware - aria_operations_for_networks	Aria Operations for Networks contains a cross site scripting vulnerability. A malicious actor with admin privileges can inject a malicious payload into the login banner and takeover the user account.	2024-02-06	4.8	Medium
CVE-2024-22386	linux - multiple products	A race condition was found in the Linux kernel's drm/exynos device driver in exynos_drm_crtc_atomic_disable() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	Medium
CVE-2024-23196	linux - multiple products	A race condition was found in the Linux kernel's sound/hda device driver in snd_hdac_regmap_sync() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	Medium
CVE-2024-24855	linux - multiple products	A race condition was found in the Linux kernel's scsi device driver in lpfc_unregister_fcf_rescan() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	Medium
CVE-2024-24864	linux - multiple products	A race condition was found in the Linux kernel's media/dvb-core in dvbdmx_write() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	Medium
CVE-2024-1312	linux - multiple products	A use-after-free flaw was found in the Linux kernel's Memory Management subsystem when a user wins two races at the same time with a fail in the mas_prev_slot function. This issue could allow a local user to crash the system.	2024-02-08	4.7	Medium
CVE-2024-20827	samsung - gallery	Improper access control vulnerability in Samsung Gallery prior to version 14.5.04.4 allows physical attackers to access the picture using physical keyboard on the lockscreen.	2024-02-06	4.6	Medium
CVE-2024-20828	samsung - internet	Improper authorization verification vulnerability in Samsung Internet prior to version 24.0 allows physical attackers to access files downloaded in SecretMode without proper authentication.	2024-02-06	4.6	Medium
CVE-2024-20016	google - multiple products	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation Patch ID: ALPS07835901; Issue ID: ALPS07835901.	2024-02-05	4.4	Medium
CVE-2023-28063	dell - optiplex_3000_micro_firmware	Dell BIOS contains a Signed to Unsigned Conversion Error vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to denial of service.	2024-02-06	4.4	Medium
CVE-2023-46183	ibm - multiple products	IBM PowerVM Hypervisor FW950.00 through FW950.90, FW1020.00 through FW1020.40, and FW1030.00 through FW1030.30 could allow a system administrator to obtain sensitive partition information. IBM X-Force ID: 269695.	2024-02-06	4.4	Medium
CVE-2023-28077	dell - multiple products	Dell BSAFE SSL-J, versions prior to 6.5, and versions 7.0 and 7.1 contain a debug message revealing unnecessary information	2024-02-10	4.4	Medium

		vulnerability. This may lead to disclosing sensitive information to a locally privileged user.			
CVE-2024-22021	veeam - multiple products	Vulnerability?CVE-2024-22021 allows?a?Veeam Recovery Orchestrator user with a low?privileged?role (Plan?Author)?to retrieve?plans?from?a?Scope other than the one they are assigned to.	2024-02-07	4.3	Medium
CVE-2023-42016	ibm - multiple products	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 265559.	2024-02-09	4.3	Medium
CVE-2024-20810	samsung - multiple products	Implicit intent hijacking vulnerability in Smart Suggestions prior to SMR Feb-2024 Release 1 allows attackers to get sensitive information.	2024-02-06	3.3	Low
CVE-2024-20811	samsung - multiple products	Improper caller verification in GameOptimizer prior to SMR Feb-2024 Release 1 allows local attackers to configure GameOptimizer.	2024-02-06	3.3	Low
CVE-2024-1048	gnu - grub2	A flaw was found in the grub2-set-bootflag utility of grub2. After the fix of CVE-2019-14865, grub2-set-bootflag will create a temporary file with the new grubenv content and rename it to the original grubenv file. If the program is killed before the rename operation, the temporary file will not be removed and may fill the filesystem when invoked multiple times, resulting in a filesystem out of free inodes or blocks.	2024-02-06	3.3	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.