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

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

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 ٢٨ يناير إلى ٣ 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

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 28th of January to 3rd 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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-6780	gnu - glibc	An integer overflow was found in the __vsyslog_internal function of the glibc library. This function is called by the syslog and vsyslog functions. This issue occurs when these functions are called with a very long message, leading to an incorrect calculation of the buffer size to store the message, resulting in undefined behavior. This issue affects glibc 2.37 and newer.	2024-01-31	9.8	Critical
CVE-2023-50940	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 275130.	2024-02-02	9.8	Critical
CVE-2023-32333	ibm - maximo_asset_management	IBM Maximo Asset Management 7.6.1.3 could allow a remote attacker to log into the admin panel due to improper access controls. IBM X-Force ID: 255073.	2024-02-02	9.8	Critical
CVE-2023-48792	zohocorp - multiple products	Zoho ManageEngine ADAudit Plus through 7250 is vulnerable to SQL Injection in the report export option.	2024-02-02	9.8	Critical
CVE-2023-48793	zohocorp - multiple products	Zoho ManageEngine ADAudit Plus through 7250 allows SQL Injection in the aggregate report feature.	2024-02-02	9.8	Critical
CVE-2024-22319	ibm - multiple products	IBM Operational Decision Manager 8.10.3, 8.10.4, 8.10.5.1, 8.11, 8.11.0.1, and 8.12.0.1 is susceptible to remote code execution attack via JNDI injection when passing an unchecked argument to a certain API. IBM X-Force ID: 279145.	2024-02-02	9.8	Critical
CVE-2023-47143	ibm - tivoli_application_dependency_discovery_manager	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.10 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: 270270.	2024-02-02	9.8	Critical
CVE-2020-29504	dell - bsafe_crypto-c-micro-edition	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain a Missing Required Cryptographic Step Vulnerability.	2024-02-02	9.8	Critical
CVE-2021-21575	dell - bsafe_micro-edition-suite	Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain an Observable Timing Discrepancy Vulnerability.	2024-02-02	9.8	Critical
CVE-2022-34381	dell - multiple products	Dell BSAFE SSL-J version 7.0 and all versions prior to 6.5, and Dell BSAFE Crypto-J versions prior to 6.2.6.1 contain an unmaintained third-party component vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to the compromise of the impacted system. This is a Critical vulnerability and Dell recommends customers to upgrade at the earliest opportunity.	2024-02-02	9.8	Critical
CVE-2023-39303	qnap - multiple products	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network.	2024-02-02	9.8	Critical

		We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later			
CVE-2023-45025	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	9.8	Critical
CVE-2023-31004	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) could allow a remote attacker to gain access to the underlying system using man in the middle techniques. IBM X-Force ID: 254765.	2024-02-03	9	Critical
CVE-2024-1059	google - chrome	Use after free in Peer Connection in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-30	8.8	High
CVE-2024-1060	google - chrome	Use after free in Canvas in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-30	8.8	High
CVE-2024-1077	google - chrome	Use after free in Network in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High)	2024-01-30	8.8	High
CVE-2024-21888	ivanti - multiple products	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.	2024-01-31	8.8	High
CVE-2023-50936	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 275116.	2024-02-02	8.8	High
CVE-2024-22320	ibm - multiple products	IBM Operational Decision Manager 8.10.3, 8.10.4, 8.10.5.1, 8.11, 8.11.0.1, and 8.12.0.1 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unsafe deserialization. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code in the context of SYSTEM. IBM X-Force ID: 279146.	2024-02-02	8.8	High
CVE-2023-38263	ibm - soar_qradar_plugin_app	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an authenticated user to perform unauthorized actions due to improper access controls. IBM X-Force ID: 260577.	2024-02-02	8.8	High
CVE-2024-0253	zohocorp - multiple products	ManageEngine ADAudit Plus versions 7270 and below are vulnerable to the Authenticated SQL injection in home Graph-Data.	2024-02-02	8.8	High
CVE-2024-0269	zohocorp - multiple products	ManageEngine ADAudit Plus versions 7270 and below are vulnerable to the Authenticated SQL injection in File-Summary DrillDown. This issue has been fixed and released in version 7271.	2024-02-02	8.8	High
CVE-2023-47142	ibm - tivoli_application_dependency_discovery_manager	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.10 could allow an attacker on the organization's local network to escalate their privileges due to unauthorized API access. IBM X-Force ID: 270267.	2024-02-02	8.8	High
CVE-2023-39297	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	8.8	High
CVE-2023-47562	qnap - photo_station	An OS command injection vulnerability has been reported to affect Photo Station. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: Photo Station 6.4.2 (2023/12/15) and later	2024-02-02	8.8	High
CVE-2023-47568	qnap - multiple products	A SQL injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	2024-02-02	8.8	High

		QTS 5.1.5.2645 build 20240116 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later			
CVE-2024-21399	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-02-02	8.3	High
CVE-2024-21893	ivanti - multiple products	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.	2024-01-31	8.2	High
CVE-2023-47564	qnap - multiple products	An incorrect permission assignment for critical resource vulnerability has been reported to affect Qsync Central. If exploited, the vulnerability could allow authenticated users to read or modify the resource via a network. We have already fixed the vulnerability in the following versions: Qsync Central 4.4.0.15 (2024/01/04) and later Qsync Central 4.3.0.11 (2024/01/11) and later	2024-02-02	8.1	High
CVE-2024-0841	linux - linux_kernel	A null pointer dereference flaw was found in the hugetlbfs_fill_super function in the Linux kernel hugetlbfs (HugeTLB pages) functionality. This issue may allow a local user to crash the system or potentially escalate their privileges on the system.	2024-01-28	7.8	High
CVE-2024-23940	trendmicro - multiple products	Trend Micro uiAirSupport, included in the Trend Micro Security 2023 family of consumer products, version 6.0.2092 and below is vulnerable to a DLL hijacking/proxying vulnerability, which if exploited could allow an attacker to impersonate and modify a library to execute code on the system and ultimately escalate privileges on an affected system.	2024-01-29	7.8	High
CVE-2024-21803	linux - multiple products	Use After Free vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (bluetooth modules) allows Local Execution of Code. This vulnerability is associated with program files https://gitee.Com/anolis/cloud-kernel/blob/devel-5.10/net/bluetooth/af_bluetooth.C. This issue affects Linux kernel: from v2.6.12-rc2 before v6.8-rc1.	2024-01-30	7.8	High
CVE-2024-1085	linux - multiple products	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The nft_setelem_catchall_deactivate() function checks whether the catch-all set element is active in the current generation instead of the next generation before freeing it, but only flags it inactive in the next generation, making it possible to free the element multiple times, leading to a double free vulnerability. We recommend upgrading past commit b1db244ffd041a49ecc9618e8feb6b5c1afcdaa7.	2024-01-31	7.8	High
CVE-2024-1086	linux - multiple products	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The nft_verdict_init() function allows positive values as drop error within the hook verdict, and hence the nf_hook_slow() function can cause a double free vulnerability when NF_DROP is issued with a drop error which resembles NF_ACCEPT. We recommend upgrading past commit f342de4e2f33e0e39165d8639387aa6c19dff660.	2024-01-31	7.8	High
CVE-2023-6246	gnu - glibc	A heap-based buffer overflow was found in the __vsyslog_internal function of the glibc library. This function is called by the syslog and vsyslog functions. This issue occurs when the openlog function was not called, or called with the ident argument set to NULL, and the program name (the basename of argv[0]) is bigger than 1024 bytes, resulting in an application crash or local privilege escalation. This issue affects glibc 2.36 and newer.	2024-01-31	7.8	High
CVE-2024-22449	dell - powerscale_onefs	Dell PowerScale OneFS versions 9.0.0.x through 9.6.0.x contains a missing authentication for critical function vulnerability. A low privileged local malicious user could potentially exploit this vulnerability to gain elevated access.	2024-02-01	7.8	High
CVE-2023-31005	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) could allow a local user to escalate their privileges due to an improper security configuration. IBM X-Force ID: 254767.	2024-02-03	7.8	High
CVE-2023-6200	linux - multiple products	A race condition was found in the Linux Kernel. Under certain conditions, an unauthenticated attacker from an adjacent network	2024-01-28	7.5	High

		could send an ICMPv6 router advertisement packet, causing arbitrary code execution.			
CVE-2023-46838	linux - linux_kernel	Transmit requests in Xen's virtual network protocol can consist of multiple parts. While not really useful, except for the initial part any of them may be of zero length, i.e. carry no data at all. Besides a certain initial portion of the to be transferred data, these parts are directly translated into what Linux calls SKB fragments. Such converted request parts can, when for a particular SKB they are all of length zero, lead to a de-reference of NULL in core networking code.	2024-01-29	7.5	High
CVE-2023-29055	apache - kylin	In Apache Kylin version 2.0.0 to 4.0.3, there is a Server Config web interface that displays the content of file 'kylin.properties', that may contain serverside credentials. When the kylin service runs over HTTP (or other plain text protocol), it is possible for network sniffers to hijack the HTTP payload and get access to the content of kylin.properties and potentially the containing credentials. To avoid this threat, users are recommended to * Always turn on HTTPS so that network payload is encrypted. * Avoid putting credentials in kylin.properties, or at least not in plain text. * Use network firewalls to protect the serverside such that it is not accessible to external attackers. * Upgrade to version Apache Kylin 4.0.4, which filters out the sensitive content that goes to the Server Config web interface.	2024-01-29	7.5	High
CVE-2023-44312	apache - servicecomb	Exposure of Sensitive Information to an Unauthorized Actor in Apache ServiceComb Service-Center.This issue affects Apache ServiceComb Service-Center before 2.1.0 (include). Users are recommended to upgrade to version 2.2.0, which fixes the issue.	2024-01-31	7.5	High
CVE-2023-44313	apache - servicecomb	Server-Side Request Forgery (SSRF) vulnerability in Apache ServiceComb Service-Center. Attackers can obtain sensitive server information through specially crafted requests.This issue affects Apache ServiceComb before 2.1.0(include). Users are recommended to upgrade to version 2.2.0, which fixes the issue.	2024-01-31	7.5	High
CVE-2023-6779	gnu - glibc	An off-by-one heap-based buffer overflow was found in the __vsyslog_internal function of the glibc library. This function is called by the syslog and vsyslog functions. This issue occurs when these functions are called with a message bigger than INT_MAX bytes, leading to an incorrect calculation of the buffer size to store the message, resulting in an application crash. This issue affects glibc 2.37 and newer.	2024-01-31	7.5	High
CVE-2023-50939	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 275129.	2024-02-02	7.5	High
CVE-2023-50326	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 275107.	2024-02-02	7.5	High
CVE-2023-50937	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 275117.	2024-02-02	7.5	High
CVE-2023-47148	ibm - spectrum_protect_plus	IBM Storage Protect Plus Server 10.1.0 through 10.1.15.2 Admin Console could allow a remote attacker to obtain sensitive information due to improper validation of unsecured endpoints which could be used in further attacks against the system. IBM X-Force ID: 270599.	2024-02-02	7.5	High
CVE-2023-38273	ibm - multiple products	IBM Cloud Pak System 2.3.1.1, 2.3.2.0, and 2.3.3.7 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 260733.	2024-02-02	7.5	High
CVE-2023-30999	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) could allow an attacker to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 254651.	2024-02-03	7.5	High
CVE-2023-31006	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) is vulnerable to a denial of service attacks on the DSC server. IBM X-Force ID: 254776.	2024-02-03	7.5	High

CVE-2023-40548	redhat - multiple products	A buffer overflow was found in Shim in the 32-bit system. The overflow happens due to an addition operation involving a user-controlled value parsed from the PE binary being used by Shim. This value is further used for memory allocation operations, leading to a heap-based buffer overflow. This flaw causes memory corruption and can lead to a crash or data integrity issues during the boot phase.	2024-01-29	7.4	High
CVE-2023-43016	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) could allow a remote user to log into the server due to a user account with an empty password. IBM X-Force ID: 266154.	2024-02-03	7.3	High
CVE-2023-5372	zyxel - nas326_firmware	The post-authentication command injection vulnerability in Zyxel NAS326 firmware versions through V5.21(AAZF.15)C0 and NAS542 firmware versions through V5.21(ABAG.12)C0 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands by sending a crafted query parameter attached to the URL of an affected device's web management interface.	2024-01-30	7.2	High
CVE-2023-39302	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41273	qnap - multiple products	A heap-based buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41275	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41276	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41277	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41278	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41279	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later	2024-02-02	7.2	High

		QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later			
CVE-2023-41280	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41281	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41282	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41283	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-41292	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-45035	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-45036	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-45037	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-47566	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions:	2024-02-02	7.2	High

		QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later			
CVE-2023-47567	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CVE-2023-40551	redhat - shim	A flaw was found in the MZ binary format in Shim. An out-of-bounds read may occur, leading to a crash or possible exposure of sensitive data during the system's boot phase.	2024-01-29	7.1	High
CVE-2023-32327	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 254783.	2024-02-03	7.1	High
CVE-2023-50359	qnap - multiple products	An unchecked return value vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local authenticated administrators to place the system in a state that could lead to a crash or other unintended behaviors via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later	2024-02-02	6.7	Medium
CVE-2024-0564	linux - linux_kernel	A flaw was found in the Linux kernel's memory deduplication mechanism. The max page sharing of Kernel Samepage Merging (KSM), added in Linux kernel version 4.4.0-96.119, can create a side channel. When the attacker and the victim share the same host and the default setting of KSM is "max page sharing=256", it is possible for the attacker to time the unmap to merge with the victim's page. The unmapping time depends on whether it merges with the victim's page and additional physical pages are created beyond the KSM's "max page share". Through these operations, the attacker can leak the victim's page.	2024-01-30	6.5	Medium
CVE-2024-21388	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-30	6.5	Medium
CVE-2023-50935	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 fails to properly restrict access to a URL or resource, which may allow a remote attacker to obtain unauthorized access to application functionality and/or resources. IBM X-Force ID: 275115.	2024-02-02	6.5	Medium
CVE-2023-46159	ibm - multiple products	IBM Storage Ceph 5.3z1, 5.3z5, and 6.1z1 could allow an authenticated user on the network to cause a denial of service from RGW. IBM X-Force ID: 268906.	2024-02-02	6.5	Medium
CVE-2023-38019	ibm - soar_qradar_plugin_app	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 260575.	2024-02-02	6.5	Medium
CVE-2023-32967	qnap - multiple products	An incorrect authorization vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to bypass intended access restrictions via a network. QTS 5.x, QuTS hero are not affected. We have already fixed the vulnerability in the following versions: QuTScloud c5.1.5.2651 and later QTS 4.5.4.2627 build 20231225 and later	2024-02-02	6.5	Medium
CVE-2023-50933	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 275113.	2024-02-02	6.1	Medium
CVE-2023-47144	ibm - tivoli_application_dependency_discovery_manager	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.10 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: 270271.	2024-02-02	6.1	Medium
CVE-2023-40546	redhat - shim	A flaw was found in Shim when an error happened while creating a new ESL variable. If Shim fails to create the new variable, it tries to print an error message to the user; however, the number of	2024-01-29	5.5	Medium

		parameters used by the logging function doesn't match the format string used by it, leading to a crash under certain circumstances.			
CVE-2023-40549	redhat - shim	An out-of-bounds read flaw was found in Shim due to the lack of proper boundary verification during the load of a PE binary. This flaw allows an attacker to load a crafted PE binary, triggering the issue and crashing Shim, resulting in a denial of service.	2024-01-29	5.5	Medium
CVE-2023-40550	redhat - shim	An out-of-bounds read flaw was found in Shim when it tried to validate the SBAT information. This issue may expose sensitive data during the system's boot phase.	2024-01-29	5.5	Medium
CVE-2024-22236	vmware - multiple products	In Spring Cloud Contract, versions 4.1.x prior to 4.1.1, versions 4.0.x prior to 4.0.5, and versions 3.1.x prior to 3.1.10, test execution is vulnerable to local information disclosure via temporary directory created with unsafe permissions through the shaded com.google.guava:guava dependency in the org.springframework.cloud:spring-cloud-contract-shade dependency.	2024-01-31	5.5	Medium
CVE-2024-22430	dell - powerscale_onefs	Dell PowerScale OneFS versions 8.2.x through 9.6.0.x contains an incorrect default permissions vulnerability. A local low privileges malicious user could potentially exploit this vulnerability, leading to denial of service.	2024-02-01	5.5	Medium
CVE-2023-32329	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.0.0 through 10.0.6.1) could allow a user to download files from an incorrect repository due to improper file validation. IBM X-Force ID: 254972.	2024-02-03	5.5	Medium
CVE-2023-50941	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 does not provide logout functionality, which could allow an authenticated user to gain access to an unauthorized user using session fixation. IBM X-Force ID: 275131.	2024-02-02	5.4	Medium
CVE-2022-40744	ibm - aspera_faspex	IBM Aspera Faspex 5.0.6 is vulnerable to stored 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: 236441.	2024-02-02	5.4	Medium
CVE-2023-51072	nagios - multiple products	A stored cross-site scripting (XSS) vulnerability in the NOC component of Nagios XI version up to and including 2024R1 allows low-privileged users to execute malicious HTML or JavaScript code via the audio file upload functionality from the Operation Center section. This allows any authenticated user to execute arbitrary JavaScript code on behalf of other users, including the administrators.	2024-02-02	5.4	Medium
CVE-2023-47561	qnap - photo_station	A cross-site scripting (XSS) vulnerability has been reported to affect Photo Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Photo Station 6.4.2 (2023/12/15) and later	2024-02-02	5.4	Medium
CVE-2023-50327	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 uses insecure HTTP methods which could allow a remote attacker to perform unauthorized file request modification. IBM X-Force ID: 275109.	2024-02-02	5.3	Medium
CVE-2023-50328	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 may allow a remote attacker to view session identifiers passed via URL query strings. IBM X-Force ID: 275110.	2024-02-02	5.3	Medium
CVE-2023-50934	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 uses single-factor authentication which can lead to unnecessary risk of compromise when compared with the benefits of a dual-factor authentication scheme. IBM X-Force ID: 275114.	2024-02-02	5.3	Medium
CVE-2023-41274	qnap - multiple products	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	Medium
CVE-2023-45026	qnap - multiple products	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later	2024-02-02	4.9	Medium

		QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later			
CVE-2023-45027	qnap - multiple products	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	Medium
CVE-2023-45028	qnap - multiple products	An uncontrolled resource consumption vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	Medium
CVE-2023-50938	ibm - multiple products	IBM PowerSC 1.3, 2.0, and 2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 275128.	2024-02-02	4.3	Medium
CVE-2023-38020	ibm - soar_qradar_plugin_app	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an authenticated user to manipulate output written to log files. IBM X-Force ID: 260576.	2024-02-02	4.3	Medium

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

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