

تمت مشاركة هذه المعلومة بإشارة مشاركة \*\*\*أبيض\*\*\* حيث يسمح بتبادلها Please note that this notification/advisory has been tagged as TLP \*\*\*WHITE\*\*\* where information can be shared or published on any public forums.

أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للتغرات المسجلة vulnerabilities by the National Institute of Standards and Technology the National Institute of Standards and Technology (NIST) من قبل (NIST) National Vulnerability Database (NVD) for the week from 28<sup>th</sup> of January to 3<sup>rd</sup> of February. Vulnerabilities are scored using the Common Vulnerability علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار 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

الله عن ۲۸ يناير إلى ۳ فبراير. National Vulnerability Database (NVD) Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

عالى جدًا: النتيجة الأساسية لـCVSS 9.0-10.0

عالى: النتيجة الأساسية لـ8.9-CVSS 7.0

متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0

منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE 2022 6780	anu aliha	An integer overflow was found in thevsyslog_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	2024 01 21	0.0	Critical
CVE-2023-6780	gnu - glibc	issue affects glibc 2.37 and newer.  IBM PowerSC 1.3, 2.0, and 2.1 uses Cross-Origin Resource Sharing	2024-01-31	9.8	Critical
CVE-2023-50940	ibm - multiple products	(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
	ibm -	IBM Maximo Asset Management 7.6.1.3 could allow a remote			
CVE-2023-32333	maximo_asset_ma nagement	attacker to log into the admin panel due to improper access controls. IBM X-Force ID: 255073.	2024-02-02	9.8	Critical
0.42.0000.40200	zohocorp - multiple	Zoho ManageEngine ADAudit Plus through 7250 is vulnerable to			
<u>CVE-2023-48792</u>	products zohocorp - multiple	SQL Injection in the report export option.  Zoho ManageEngine ADAudit Plus through 7250 allows SQL	2024-02-02	9.8	Critical
CVE-2023-48793	products	Injection in the aggregate report feature.	2024-02-02	9.8	Critical
	ibm - multiple	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			
CVE-2024-22319	products	a certain API. IBM X-Force ID: 279145.	2024-02-02	9.8	Critical
CVE-2023-47143	ibm - tivoli_application_d ependency_discove ry_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
CVL-2023-33303	products	<u>l</u>	2024-02-02	9.0	Citical

	T				ı
		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  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			
CVE-2023-45025	qnap - multiple products	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 2022 24004	ibm - multiple	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	2024 02 02	0	Cuiking
CVE-2023-31004	products	middle techniques. IBM X-Force ID: 254765.  Use after free in Peer Connection in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit	2024-02-03	9	Critical
CVE-2024-1050	google - chrome	stack corruption via a crafted HTML page. (Chromium security	2024-01-20	QQ	High
CVE-2024-1059	google - chrome	severity: High)  Use after free in Canvas in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption	2024-01-30	8.8	High
CVE-2024-1060	google - chrome	via a crafted HTML page. (Chromium security severity: High)	2024-01-30	8.8	High
		Use after free in Network in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit			
CVE-2024-1077	google - chrome	heap corruption via a malicious file. (Chromium security severity: High)	2024-01-30	8.8	High
		A privilege escalation vulnerability in web component of Ivanti			
CVE-2024-21888	ivanti - multiple products	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
	ibm - multiple	IBM PowerSC 1.3, 2.0, and 2.1 does not invalidate session after logout which could allow an authenticated user to impersonate			
CVE-2023-50936	products	another user on the system. IBM X-Force ID: 275116.	2024-02-02	8.8	High
		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			
	ibm - multiple	deserialization. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code in the			
CVE-2024-22320	products ibm -	context of SYSTEM. IBM X-Force ID: 279146.  IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an	2024-02-02	8.8	High
CVE-2023-38263	soar_qradar_plugin _app	authenticated user to perform unauthorized actions due to improper access controls. IBM X-Force ID: 260577.	2024-02-02	8.8	High
	zohocorp - multiple	ManageEngine ADAudit Plus versions 7270 and below are vulnerable to the Authenticated SQL injection in home Graph-			
CVE-2024-0253	products	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
<u> </u>	ibm -	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0	2027 02 02	0.0	111811
0.45 - 2.5 -	tivoli_application_d ependency_discove	through 7.3.0.10 could allow an attacker on the organization's local network to escalate their privileges due to unauthorized API	0000		
CVE-2023-47142	ry_manager	access. IBM X-Force ID: 270267.  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	2024-02-02	8.8	High
		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			
CVE-2023-39297	qnap - multiple products	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
CAT 7072-22721	products	An OS command injection vulnerability has been reported to affect	202 <del>1</del> -02-02	0.0	i iigii
		Photo Station. If exploited, the vulnerability could allow authenticated users to execute commands via a network.			
CVE-2023-47562	qnap - photo_station	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
		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.			
CVE 2022 47500	qnap - multiple		2024.02.02	0.0	11:-1-
CVE-2023-47568	products	We have already fixed the vulnerability in the following versions:	2024-02-02	8.8	High

	T	OTC 5 4 5 2045 h wild 20240440 and laten			
		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	∐iah
CVE-2024-21399	euge_ciiroimum	A server-side request forgery vulnerability in the SAML component	2024-02-02	0.5	High
		of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x,			
	ivanti - multiple	22.x) and Ivanti Neurons for ZTA allows an attacker to access			
CVE-2024-21893	products	certain restricted resources without authentication.	2024-01-31	8.2	High
		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:			
CVE-2023-47564	qnap - multiple products	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
CVL-2023-47304	products	A null pointer dereference flaw was found in the	2024-02-02	0.1	riigii
		hugetlbfs_fill_super function in the Linux kernel hugetlbfs			
		(HugeTLB pages) functionality. This issue may allow a local user to			
0.45 2024 0044		crash the system or potentially escalate their privileges on the	2024 04 22	7.0	
CVE-2024-0841	linux - linux_kernel	system.  Trend Micro uiAirSupport, included in the Trend Micro Security	2024-01-28	7.8	High
		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			
CVE 2024 22040	trendmicro -	library to execute code on the system and ultimately escalate	2024 04 20	7.0	LU: ede
CVE-2024-23940	multiple products	privileges on an affected system.  Use After Free vulnerability in Linux Linux kernel kernel on Linux,	2024-01-29	7.8	High
		x86, ARM (bluetooth modules) allows Local Execution of Code.			
		This vulnerability is associated with program files			
		https://gitee.Com/anolis/cloud-kernel/blob/devel-			
	linux - multiple	5.10/net/bluetooth/af_bluetooth.C.			
CVE-2024-21803	products	This issue affects Linux kernel: from v2.6.12-rc2 before v6.8-rc1.	2024-01-30	7.8	High
072 202 1 21000	products	A use-after-free vulnerability in the Linux kernel's netfilter:	20210130	7.0	6
		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.			
	linux - multiple	We recommend upgrading past commit			
CVE-2024-1085	products	b1db244ffd041a49ecc9618e8feb6b5c1afcdaa7.	2024-01-31	7.8	High
		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.			
	linux - multiple	We recommend upgrading past commit			
CVE-2024-1086	products	f342de4e2f33e0e39165d8639387aa6c19dff660.	2024-01-31	7.8	High
		A heap-based buffer overflow was found in thevsyslog_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.			
CVE-2023-6246	gnu - glibc	This issue affects glibc 2.36 and newer.	2024-01-31	7.8	High
		Dell PowerScale OneFS versions 9.0.0.x through 9.6.0.x contains a			
		missing authentication for critical function vulnerability. A low			
	dell -	privileged local malicious user could potentially exploit this			
CVE-2024-22449	powerscale_onefs	vulnerability to gain elevated access.	2024-02-01	7.8	High
		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			
	ibm - multiple	to escalate their privileges due to an improper security			
CVE-2023-31005	products	configuration. IBM X-Force ID: 254767.	2024-02-03	7.8	High
	linux - multiple	A race condition was found in the Linux Kernel. Under certain			
CVE-2023-6200	products	conditions, an unauthenticated attacker from an adjacent network	2024-01-28	7.5	High

	T			1	
		could send an ICMPv6 router advertisement packet, causing			
		arbitrary code execution.  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			
CVE-2023-46838	linux - linux_kernel	zero, lead to a de-reference of NULL in core networking code.	2024-01-29	7.5	High
		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.			
		T			
		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			
CVE-2023-29055	apache - kylin	sensitive content that goes to the Server Config web interface.	2024-01-29	7.5	High
		Exposure of Sensitive Information to an Unauthorized Actor in			
		Apache ServiceComb Service-Center.This issue affects			
		Apache ServiceComb Service-Center			
		7,644.16			
		before 2.1.0 (include).			
	apache -	Users are recommended to upgrade to version 2.2.0, which fixes			
CVE-2023-44312	servicecomb	the issue.	2024-01-31	7.5	High
		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 Service Comb before 2.1.0(include).			
		Apache Service comb before 2.1.0(include).			
	apache -	Users are recommended to upgrade to version 2.2.0, which fixes			
CVE-2023-44313	servicecomb	the issue.	2024-01-31	7.5	High
		An off-by-one heap-based buffer overflow was found in thevsyslog_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			
CVE-2023-6779	gnu - glibc	the message, resulting in an application crash. This issue affects glibc 2.37 and newer.	2024-01-31	7.5	High
<u> </u>	Pina Pinac	IBM PowerSC 1.3, 2.0, and 2.1 uses weaker than expected	202 7 01 01	,	111811
	ibm - multiple	cryptographic algorithms that could allow an attacker to decrypt			
CVE-2023-50939	products	highly sensitive information. IBM X-Force ID: 275129.	2024-02-02	7.5	High
	ibm - multiple	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			
CVE-2023-50326	products	credentials. IBM X-Force ID: 275107.	2024-02-02	7.5	High
	,	IBM PowerSC 1.3, 2.0, and 2.1 uses weaker than expected		-	<u> </u>
0) (5, 2222 - 55-5-	ibm - multiple	cryptographic algorithms that could allow an attacker to decrypt	2024 55 55		
CVE-2023-50937	products	highly sensitive information. IBM X-Force ID: 275117.  IBM Storage Protect Plus Server 10.1.0 through 10.1.15.2 Admin	2024-02-02	7.5	High
		Console could allow a remote attacker to obtain sensitive			
	ibm -	information due to improper validation of unsecured endpoints			
OVE 2000 177	spectrum_protect_	which could be used in further attacks against the system. IBM X-	2024 25 55		
CVE-2023-47148	plus	Force ID: 270599.  IBM Cloud Pak System 2.3.1.1, 2.3.2.0, and 2.3.3.7 uses an	2024-02-02	7.5	High
		inadequate account lockout setting that could allow a remote			
	ibm - multiple	attacker to brute force account credentials. IBM X-Force ID:			
CVE-2023-38273	products	260733.	2024-02-02	7.5	High
		IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and 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			
	ibm - multiple	to cause a denial of service due to uncontrolled resource			
CVE-2023-30999	products	consumption. IBM X-Force ID: 254651.	2024-02-03	7.5	High
		IBM Security Access Manager Container (IBM Security Verify			
	ibm - multiple	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			
CVE-2023-31006	products	of service attacks on the DSC server. IBM X-Force ID: 254776.	2024-02-03	7.5	High
3_5 5_500	1				

		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			
	redhat - multiple	corruption and can lead to a crash or data integrity issues during			
CVE-2023-40548	products	the boot phase.	2024-01-29	7.4	High
		IBM Security Access Manager Container (IBM Security Verify			
		Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify			
	ibm - multiple	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			
CVE-2023-43016	products	password. IBM X-Force ID: 266154.	2024-02-03	7.3	High
<u>CVL 2023 13010</u>	products	The post-authentication command injection vulnerability in Zyxel	20210203	7.5	1.1.611
		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			
0.45 0000 5050	zyxel -	parameter attached to the URL of an affected device's web			
CVE-2023-5372	nas326_firmware	management interface.	2024-01-30	7.2	High
		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.			
		Communas via a network.			
		We have already fixed the vulnerability in the following versions:			
		QTS 5.1.3.2578 build 20231110 and later			
	qnap - multiple	QuTS hero h5.1.3.2578 build 20231110 and later			
CVE-2023-39302	products	QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
		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.			
		code via a network.			
		We have already fixed the vulnerability in the following versions:			
		QTS 5.1.2.2533 build 20230926 and later			
	qnap - multiple	QuTS hero h5.1.2.2534 build 20230927 and later			
CVE-2023-41273	products	QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
		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.			
		NA/a haya alina di filipadaha ayaha kata in Aha fallaying yanisana			
		We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later			
	gnap - multiple	QuTS hero h5.1.2.2534 build 20230927 and later			
CVE-2023-41275	products	QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
	P	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:			
	anan multinla	QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later			
CVE-2023-41276	qnap - multiple products	QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
CV L-2023-412/0	products	A buffer copy without checking size of input vulnerability has been	202 <del>4</del> -02-02	1.4	ıııgıı
		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			
0) (#. 222-	qnap - multiple	QuTS hero h5.1.2.2534 build 20230927 and later	0.55 ( -		
CVE-2023-41277	products	QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
		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.			
		and the state of the checked code vid a network.			
		We have already fixed the vulnerability in the following versions:			
		QTS 5.1.2.2533 build 20230926 and later			
	qnap - multiple	QuTS hero h5.1.2.2534 build 20230927 and later			
CVE-2023-41278	products	QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	High
		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.			
	gnan - multiple	We have already fixed the vulnerability in the following versions:			
CVE-2023-41279	qnap - multiple products	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			
		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.			
CV5 2022 44200	qnap - multiple	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	2024 02 02	7.0	ne. I
CVE-2023-41280	products	An OS command injection vulnerability has been reported to affect	2024-02-02	7.2	High
		several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network.			
CVE-2023-41281	qnap - multiple products	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
		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.			
CVE-2023-41282	qnap - multiple products	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
	product	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.			***************************************
CVE-2023-41283	qnap - multiple products	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
		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:			
CVE-2023-41292	qnap - multiple products	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
		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.			
CVE-2023-45035	qnap - multiple products	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
		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.			
CVE-2023-45036	qnap - multiple products	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
	·	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.			J
CVE-2023-45037	qnap - multiple products	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
		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.			<b>0</b>
CVE-2023-47566	qnap - multiple products	We have already fixed the vulnerability in the following versions:	2024-02-02	7.2	High

IBM Security Access Manager Container (IBM Security Verify Access Docker 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 (XXV 21 stack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 2024-02-03 7.1 High Process of Control of State State (Verify Access Docker 10,0.0.0 through 10.0.6.1) is vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 2024-02-03 7.1 High Process of Control of State State (Verify Could allow oat 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 5.1.5.645 build 20240118 and later QUTS hero 15.1.5.2647 build 20240118 and later 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 unmay to merge with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on the victim's wel			QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later			
several CNAP operating system versions, if exploited, the vulnerability could allow authenticated administrators to securite commands via a network.  We have already fixed the vulnerability in the following versions: 0755-15-1656 bould 2020/0156 mil terr QUTS-bould 2020/0156			QuTScloud c5.1.5.2651 and later			
vulnerability could allow authenticated administrators to execute commands via a network.  We have already fixed the vulnerability in the following versions: Q15 s.1.2.845 sould 2020-015 and later Q15 sould 2020-015			1			
Commands via a network.  We have already fixed the vulnerability in the following versions: OTS 5.15.2665 build 20240116 and later OTS 4.4.070 huild 20231273 and later OTS 5.15.2665 build 20240116 and later OTS 4.4.070 huild 20231273 and later OTS 5.15.2665 build 20240116 and later OTS 5.15.2665 build 20240125 build place and build bu			· · · · · · · · · · · · · · · · · · ·			
We have already fixed the vulnerability in the following versions: CITS 5.1.5245 build 2024125 and later QUTS for 16.1.5 2647 build 2024125 and later QUTS for 16.1.5 2651 build 20240116 build 2024012 buil						
OTS 5.1.5.468 build 2021/215 and later   OUTS 6.1.5.7647 build 2021/215 and 1804 because you have a considerable of the			Commanus via a network.			
CVE-2023-47567 products of USS here 16.1.5.2647 build 20231223 and later of CVF-2023-47567 products of USS here 16.1.5.2647 build 20231273 and later of CVF-2023-40551 reduct - she has -5.265 build 20231273 and later of CVF-2023-40551 reduct - she has -5.265 build 20231273 and later of CVF-2023-40551 reduct - she has -5.265 build 20231273 and later of CVF-2023-40551 reduct - she has -5.265 build 20231273 and later of CVF-2023-40551 reduct - she has -5.265 build 20231273 boild promise in Shim. An out-of-following the System's boot phose of the Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Verify Access Appliance (10.0.0.0 brough 10.0.0.1 and IBM Security Access Appliance (10.0.0 brough 10.0.0.1 and IBM Security Access Appliance (10.0.0 brough 10.0.0.1 and IBM Security Access (10.0.0 brough 10.0.0 brough 10.0.0 and IBM Security Access (10.0.0 brough 10.0.0 and IBM Security Access (10.0.0 brough 10.0.0 and IBM Security Access (10.0.0 brough 10.0 and IBM Security A			We have already fixed the vulnerability in the following versions:			
Quit   Serve   16.1.5.   2,6247 build   2021/23 and later   Quit   2024 0.12 and later   2024 0			QTS 5.1.5.2645 build 20240116 and later			
QuisSeduet Sci. 3.5 as an absence of the products of the produ						
CVE-2023-40552 products   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 sensible data during the system bot ophases.   2024-01-29   7.1   High Secrity Access Decker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and little Security Verify Access Docker 10.0.0 through 10.0.6.1 and little Verify Access Docker 10.0.0 through 10.0.6.1 and little Verify Verify Access Docker 10.0.0 through 10.0.6.1 and little Verify Verify Access Docker 10.0.0 through 10.0.6.1 and little Verify Verify Access Docker 10.0.0 through 10.0.6.1 and little Verify Verify Verify Access Docker 10.0.0 through 10.0.6.1 and little Verify						
A flaw was found in the Mz binary format in Shim. An out-of bounds read may occur, leading to a crash or possible seposure of sensitive data during the system's boot phase.  If MS Security Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0.00 through 10,0.6.1 and IBM Security Verify Access Appliance 10,0.00 through 10,0	CVE 2022 47567			2024 02 02	7.2	11:
bounds read may occur, leading to a crash or possible exposure of software that shim is ensistive data during the systems both phase.    BM Security Access Manager Container (BM Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and BM Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and BM Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and BM Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and BM Security Verify Access Docker 10.0.0.0 through 10.0.6.1 and BM Security Verify Access Docker 10.0.0.0 through 10.0.6.1 by swinerable to a NML External Entity injection (XXP.1 stack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. BBM X-Force ID: 2924-07.03 7.1 High Phase Process Committed and Phase Process Could allow local authenticated administrators to place the system in a state that could lead to a crash or other unintended behaviors wan suspecified vectors.    We have already fixed the vulnerability in the following versions: QTS 5.15.2645 build 20240118 and later QUIS hero 95.15.2648 build 2024018 and later QUIS hero 95.2648 build 2024018 bui	CVE-2023-47567	products	-	2024-02-02	7.2	High
CVE-2023-40551   redinat - shim   Secretive data during the system's boot phase.   2024-01-29   7.1   high			,			
IBM Security Access Manager Container (IBM Security Verify Access Pocker 10.0.0.6 through 10.6.6.1 and IBM Security Verify Access Application (10.0.6.1) and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker 10.0.0.0 through 10.6.6.1 and IBM Security Verify Access Pocker Could educed to Access responsibly to expose sensitive information on consume memory resources. IBM X-Force ID: 2024-02-03 7.1 lright of the Verification of the Verification of IBM Security Verify Access Pocker Could and IBM Security Verify Access Pocker Could and IBM Security Verify Access Pocker Could and IBM Security Verify Access Pocker Could Security Verify Very Verify Access Pocker Could Security Verify Very Verify Access Pocker Could Security Verify Very Verify Verify Could Security Verify Very Verify Verify Verify Verify Verify Verify Very Verify Verif	CVE-2023-40551	redhat - shim		2024-01-29	7.1	High
Access Docker 10.0.0.0 through 10.0.6.1) is wilnerabilit to an XML External First in plaction (NEP) tatack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. BMN Feore ID: 2074-02-03 7.1 High  An unchecked return value vulnerability has been reported to affect several (NAP aperating 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 5.15.2658 build 20240118 and later QUTS here followed in the Linux kernel's memory deduplication mechanism. The max page sharing of Kernel Samenage Merging (ISM), added in Linux kernel version 4.0-96.119, can create a side channel. When the attacker and the victum share the same host and the default setting of ISM 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 sharing-156"; 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 sharing-156"; 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 sharing-156"; it is possible for the attacker to make the victim's page.  QVE-2024-21388  edge_chronium  ibm multiple  ibmmultiple  ibmmultiple  ibmmultiple  ibmmultiple  ibmmultiple  ibmmultiple  ibmmultiple  quapmultiple  quapmultiple  quapmultiple  quapmultiple  quapmultiple  quapmultiple  quapmultiple  q						
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.  An unchecked return value vulnerability has been reported to affect several ONAP operating system versions in 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.  VE 2023-50359 products  QTS 5.1.5.2645 build 20240113 and later contains the hard several position of the vinnerability 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.  VE 2023-50359 products  A flaw was round in the litux kernel's memory deduplication mechanism. The may page sharing of Kernel Samegage Merging (XSM), added in litux kernel's Memory deduplication mechanism. The may page sharing of Kernel Samegage sharing 25°, it is possible for the attacker to time the uninsp to merge with the victim's page. The unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page and additional physical pages are created beyond the KSM. "man page sharing." 25°, it is possible for the attacker to time the uninsp to merge with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depends on whether it merges with the victim's page. Plan unmapping time depen			Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify			
ibm - multiple  VVE-2023-32327  products  An unchecked return value vulnerability to expose sensitive information or consume memory resources. IBM N-Force ID: 2024-02-03 7.1 High products  An unchecked return value vulnerability has been reported to affect several ONAP 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: CTS 1.5.2645 bails 1202/40118 and later  A flaw was found in the lumax kernel smemory deduplication mechanism. The max page sharing of Kernel Samepage Merging (KSM), added in Linux kernel version 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 unimap to merges with the victim's page. The unimapping time depends on whether it merges with the victim's page. The unimapping time depends on whether it merges with the victim's page and additional physical pages are created beyond the KSMs" max page sharing. 256", it is possible for the attacker can leak the victim's page.  CVE-2024-0564 Imux - Imux kernel Microsoft Edge (Chromium Sedge) [Leventon of Privilege Victim's page and additional physical pages are created beyond the KSMs" max page sharing. 256", it is microsoft to the attacker can leak the victim's page.  CVE-2024-0564 [Inux - Imux kernel] Microsoft Edge (Chromium Sedge) [Leventon of Privilege Victim's page and additional physical pages are created beyond the KSMs" max page sharing. 256", it is microsoft.  CVE-2024-0565 [Inux - Imux kernel] Microsoft Edge (Chromium Sedge) [Leventon of Privilege Victim's page and page of Privilege Victim's page and page of Privilege Victim's page and page of Privilege Victim's page (Chromium Sedge) [Leventon Sedge (Chromium Sedge) [Leventon Sedge (Chromium Sedge) [Leventon Sedge) [Leven			<u> </u>			
timer-multiple products   254783.			1			
CVE-2023-32327 products 2.54783. 2024-02-03 7.1 High An unchecked return value vulnerability has been reported to affect several QNAP operating system wersions. 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-5.1.5,2645 build 20240118 and later QUTS-6.1.5,2645 build 2024012 b		96 102 . 1 .	1			
An unchecked return value vulnerability has been reported to affect several ONAP operating system wersions. 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: QUES 1.5.2645 pould 20240116 and later QUES 1.5.2645 pould 20240116 and later 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's memory deduplication mechanism. The max page sharing of Kernel Samepage Merging (KSM), added in Linux kernel version 4.4.9.96.119, can create a side channel. When the attacker and the victim share the same host and the default setting of KSMIs' max page sharing=256°, it is possible for the attacker to time the unmap to merge with the victim's page and additional physical pages are created beyond the KSMIs' max page share'. Through these operations, the attacker can leak the victim's page and additional physical pages are created beyond the KSMIs' max page share'. Through these operations, the attacker can leak the victim's page and additional physical pages are created beyond the KSMIs' max page share'. Through these operations, the attacker can leak the victim's page.  QUE 2024-0130	CVE 2022 2227	•	•	2024 02 02	7 1	⊔iah
affect several ONAP operating system versions. If expolited, 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 QUIS from the Court of the Ward of the Court of	CVE-2023-32321	products		2024-02-03	7.1	підіі
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-51-52-645 bioliz 02040116 and later QuTS hero h5.1-5.2647 build 20240118 and later QuTS hero h5.1-5.2647 build 20240118 and later QuTS hero h5.1-5.2647 build 20240118 and later 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 KSMs' "max page sharing=256", it is possible for the attacker to time the unmap to merge with the victim's page and additional physical pages are created beyond the KSMs' "max page share". Through these operations, the attacker can leak the victim's page and additional physical pages are created beyond the KSMs' "max page share". Through these operations, the attacker can leak the victim's page and additional physical pages are created beyond the KSMs' "max page share". Through these operations, the attacker can leak the victim's page.  QVE-2024-0564 Inux - linux kernel Ibm - multiple Ibm						
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 20240115 and later QUTS hero 15.1.5.2647 build 20240116 and later QUTS hero 15.1.5.2647 build 20240118 memory deduplication mechanism. The max page sharing of Kemis Bameapage Merging (KISM), added in Limux kernel whost and the defaults testing of KSM is "max page sharing-15.56"; it is possible for the attacker to 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 sharing-15.7.50"; the state of the state of the victim's page and additional physical pages are created beyond the KSM's "max page sharing through these operations, the attacker to the victim's page.  QUE-2024-0564 limux - limux, kernel microsoft Edge (Chromium-based) Elevation of Privilege VVE-2024-0585 products  IBM PowerSC 1.3. 2.0, and 2.1 fails to properly restrict access to a outle of the victim's page.  QUE-2023-05935 products  IBM Storage Ceph 5.321, 5.325, and 6.121 could allow a remote attacker to resource, which may allow a remote attacker to the network to cause a denial of service from RGW. IBM X-Force ID: 256906.  IBM Storage Ceph 5.321, 5.325, and 6.121 could allow a remote attacker to traverse directories on the system. An attacker could send a specially credue URL resource to could send a specially credue URL resource to the special products  QUE-202			· · · · · · · · · · · · · · · · · · ·			
We have already fixed the vulnerability in the following versions: QTS 5.15.2645 build 20240118 and later QTS 5.15.2645 build 20240118 and later QUTS hero hS 1.5.2646 build 20240118 and later QUTS hero hS 1.5.2647 build 20240118 and later A llaw was found in the Linux kernel's memory deduplication mechanism. The max page sharing of Krend 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 hots and the default setting of KSM is "max page sharing-556", 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 sharing-Through these operations, the attacker can leak the victim's page.  CVE-2024-0564 linux - linux kernel microsoft - the control of the KSM's "max page sharing-timough the control of the cont						
CVE-2023-50359 products  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 varies of A-4.0-56.119, 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 sharel". Through these operations, the microsoft with the victim's page and additional physical pages are created beyond the KSM's "max page sharel". Through these operations, the attacker can leak the victim's page.  CVE-2024-21388 edge, chromium based) Elevation of Privilege  Viered and the microsoft and the state of the common of the state of the st			unintended behaviors via unspecified vectors.			
OVE-2023-50359 products  OTS 5-1.5.2645 build 20240118 and later  OUTS bero ISh.1.5.2645 build 20240118 and later  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 4.4-05-6.119, 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 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 microsoft - dege (chromium-based) Elevation of Privilege  OVE-2024-21388 edge, chromium with the victim's page.  OVE-2024-21388 edge, chromium based) Elevation of Privilege  OVE-2023-50935   BIM PowerSC 1.3, 2.0, and 2.1 falls 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 Storage Ceph 5.321, 5.35, and 6.121 could allow an authenticated user on the network to cause a denial of service from RGW. IBM X-Force ID: 258906.  OVE-2023-46159   BM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow a authenticated user on the network to cause a denial of service from RGW. IBM X-Force ID: 258906.  OVE-2023-38019   BM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an authenticate duser on the network to cause a denial of service from RGW. IBM X-Force ID: 258906.  OVE-2023-38019   BM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an authenticate of the system. IBM X-Force Discovery Marchae and the could send a specially crafted URL request containing "dot dot" sequences (J./1) to lew arthorization vulnerability in the following versions: QUEX-02-02   6.5 Medit IBM Tower ID: 2569575.  OVE-2023-50933						
QUES 2023-50359 products   QuTS hero IS. 1.5.2647 build 20240118 and later   2024-02-02   6.7   Media   A flaw was found in the Linux kernel's memory deduptication 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. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges with the victim's page. The unmapping time depends on whether it merges 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   Media of the victim share of the continual time of the victim's page. 2024-01-30   6.5   Media of the victim share of the victim's page. 2024-01-30   6.5   Media of the victim share of the victim's page. 2024-01-30   6.5   Media of the victim share of the victim's page. 2024-01-30   6.5   Media of the victim share o			, , , , , , , , , , , , , , , , , , , ,			
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 4.4.9-96.119, 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 KSMs" smax page share". Through these operations, the attacker can leak the victim's page and additional physical pages are created beyond the KSMs" smax page share". Through these operations, the attacker can leak the victim's page.  CVE-2024-21388 edge, chromium varies page.  IBM PowerSC I.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 Shorage Ceph 5.321, 5.325, and 6.121 could allow an authenticated user on the network to cause a denial of service from RGW. IBM X-Force ID: 258906.  CVE-2023-46159 IBM SOAR QRadar Plugin App 1.0 through 5.03 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (./.1) to view arbitrary files on the system. IBM X-Force Dic. 269375.  CVE-2023-38019 An incorrect authorization vulnerability in the following versions: Quit-Soud 6.5. Medic affect several QNAP operating system versions. If exploited, the vulnerability could allow an authorized system of the vulnerability could allow an authorized system versions in exploited, the vulnerability could allow attending "dot dot" sequences (./.1) to view arbitrary files on the system. IBM X-Force Dic. 269375.  An incorrect authorization vulnerability in the following versions: Quit-Soud 6.5. Medic IBM Powers Cl.3, 2.0, and 2.1 is vulnerability to the following versions: Quit-Soud 6.5. Medic IBM Po	CVE 2022 F02F0			2024 02 02	6.7	NA - d'
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.  CVE-2024-0564 linux - linux_kernel emicrosoft dege_chromium-based) Elevation of Privilege volunerability on the victim's page.  CVE-2023-50935 products libm - multiple ibm - multiple coverage ibm - multiple products libm - multiple coverage volunerability on the volunerability on the victim's page.  CVE-2023-46159 products libm - multiple products libm - soar_gradar_plugin products ibm - soar_gradar_plugin products libm - soar_gradar_plugin pap libm - volunerability out of the volunerability out of the volunerability volunerability volunerability volunerability volunerability out of war of the volunerability volunerability volunerability out of the volunerability volunerability volunerability out of low are not affected.  We have already fixed the vulnerability in the following versions: Qu75-0-02 6.5 Medic vulnerability could allow authenticated users to bypass intended access restrictions via a network. Qu75-s., 2012-0-02 6.5 Medic vulnerability could allow authenticated users to bypass intended access restrictions via a network. Qu75-s., 2012-0-02 6.5 Medic vulnerability out of labor vu	CVE-2023-50359	products	1	2024-02-02	6.7	Mediun
(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.  CVE-2024-0130  CVE-2024-21388    Inux - Iniux_kernel   microsoft - edge_chromium   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Media			1			
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. 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.  CVE-2024-01-30 6.5 Medit Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability 2024-01-30 6.5 Medit 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 Storage Ceph 5.321, 5.325, and 6.121 could allow an unauthorized access to application functionality and/or resource access to application functionality and access to application and access resource access to application functionality and access to application and access to application functional access to application and access to application functional provided access to access to application functional provided access to application functional provided access to application functional provided acc			, , , , , , , , , , , , , , , , , , , ,			
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.  CVE-2024-21388   microsoft - edge_chromium   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2024-21388   microsoft - edge_chromium   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2023-50935   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2023-50935   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2023-50935   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2023-46159   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2023-46159   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-01-30   6.5   Medit    CVE-2023-46159   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-46159   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-38019   microsoft   Microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-38019   microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-38019   microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-38019   microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-38019   microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-38019   microsoft Edge (Chromium-based) Elevation of Privilege   2024-02-02   6.5   Medit    CVE-2023-3903   microsoft Edge (Chromium-based) Elevation of Privile						
victim's page. The ummapping 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.  OVE-2024-21388 edge chromium dicrosoft Edge (Chromium-based) Elevation of Privilege (2024-01-30) 6.5 Medit (2024-21388) edge chromium dicrosoft Edge (Chromium-based) Elevation of Privilege (2024-01-30) 6.5 Medit (2024-21388) edge chromium dible (2024-21388) edge chromium displant (2024-21388) edge chro			host and the default setting of KSM is "max page sharing=256", it			
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.  Wicrosoft Edge (Chromium-based) Elevation of Privilege  Wilerability  Dim - 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 Storage Ceph S.321, S.325, and 6.121 could allow an authenticated user on the network to cause a denial of service from RGW. IBM X-Force ID: 268906.  CVE-2023-46159  IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow a remote attacker to traverse directories on the system. IBM X-Force ID: 268906.  CVE-2023-38019  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 (J1) to view arbitrary files on the system. IBM X-Force ID: 268906.  CVE-2023-38019  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:  QTS-5.x, QuTS hero are not affected.  We have already fixed the vulnerability in the following versions:  QTS-5.x, QuTS hero are not affected.  We have already fixed the vulnerability in the following versions:  QTS-5.x, QuTS hero are not affected.  We have already fixed the vulnerability in the following versions:  QTS-5.x, QuTS hero are not affected.  We have already fixed the vulnerability in the following versions:  QTS-5.x, QuTS hero are not affected.  We have already fixed the vulnerability in the following versions:  QTS-5.x, QuTS hero are not affected.  We have already fixed the vulnerability in the following versions:  QTS			is possible for the attacker to time the unmap to merge with the			
beyond the KSM's "max page share". Through these operations, the attacker can leak the victim's page.    Microsoft - Winerability   Winerabil						
CVE-2024-0564 linux - linux_kernel microsoft - microsoft - dege_chromium - dege_chromium - dege_chromium - dultiple products   libm - multiple products   libm - motion   libm - multiple products   libm - motion   lib						
microsoft - edge chromium - Microsoft Edge (Chromium-based) Elevation of Privilege - 2024-01-30 6.5 Mediu - Edge chromium - Ed	CVE 2024 0564	Barre Barre Lamas		2024 04 20	6.5	N A maliana
CVE-2023-3035 edge_chromium	CVE-2024-0564	_		2024-01-30	6.5	iviediuri
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.   2024-02-02   6.5   Media	CVE-2024-21388			2024-01-30	6.5	Medium
ibm - multiple products   IBM X-Force ID: 275115.   IBM X-Force ID: 275115.   2024-02-02   6.5   Medit unauthorized access to application functionality and/or resources.   2024-02-02   6.5   Medit IBM X-Force ID: 275115.   IBM X-Force ID: 275115.   2024-02-02   6.5   Medit IBM X-Force ID: 275115.   IBM X-Force ID: 275115.   2024-02-02   6.5   Medit IBM X-Force ID: 275023-46159   IBM X-Force ID: 268906.   2024-02-02   6.5   Medit IBM X-Force ID: 269575.   2024-02-02   6.5   Medit IBM X-Force ID: 27513.   2024-02-02   6.1   Medit IBM X-Force ID: 270271.   A flaw was found in Shim when an error happened while creating a			•			
CVE-2023-50935 products IBM X-Force ID: 275115. 2024-02-02 6.5 Media ibm - multiple products ibm - multiple products   IBM Storage Ceph 5.321, 5.325, and 6.121 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 Media   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 Media   IBM correct 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 Media   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 Media   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: 2024-02-02 6.1 Media   A flaw was found in Shim when an error happened while creating a						
IBM Storage Ceph 5.321, 5.325, and 6.121 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   Media		ibm - multiple	unauthorized access to application functionality and/or resources.			
ibm - multiple products from RGW. IBM X-Force ID: 268906.  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.  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  QTS 4.5.4.2627 build 20231225 and later  QTS 4.5.4.2627 build 20231225 and later  ibm - multiple ibm - multiple viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 275113.  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 tivoli_application_d ependency_discove ry_manager  CVE-2023-47144 ry_manager  A flaw was found in Shim when an error happened while creating a	CVE-2023-50935	products		2024-02-02	6.5	Mediun
Section   CVE-2023-46159   products   from RGW. IBM X-Force ID: 268906.   2024-02-02   6.5   Media   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   Media   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   Media   Med			· · · · · · · · · · · · · · · · · · ·			
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.  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  QTS 4.5.4.2627 build 20231225 and later  BM Power SC 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.  BM 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 credentialls disclosure within a trusted session. IBM X-Force ID: 2024-02-02 6.1 Medic VE-2023-47144 Pagnanager  CVE-2023-47144 A flaw was found in Shim when an error happened while creating a	CVE 2022 464E0	•		2024 02 02	6.5	N A m alii
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 Discrete 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 QUSCOURT 4.5	CVE-2023-46159	products		2024-02-02	6.5	ivieaiun
ibm - soar_gradar_plugin			1			
soar_qradar_plugin _app   Sequences (/./) to view arbitrary files on the system. IBM X-Force   ID: 260575.   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:   QuTS cloud c5.1.5.2651 and later   QTS 4.5.4.2627 build 20231225 and later   QUZ4-02-02   6.5   Media   DEC 4.5.4.2627 build 20231225 and later   QTS 4.5.4.2627 build 20231225 and later   QUZ4-02-02   CZ4-02-02   CZ4-02-02   CZ4-02-02   DEC 4.5.4.2627 build 20231225 and later   QTS 4.5.4.2627 build 20231225 and later   QUZ4-02-02   DEC 4.5.4.2627 build 20231225 and later   DEC 4.5.4.2627 build 20231225 and later   QUZ4-02-02   DEC 4.5.4.2627 build 20231225 and later   DEC 4.5.4.2627 build 20231225 and late		ibm -	,			
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  QTS 4.5.4.2627 build 20231225 and later  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.  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: 2024-02-02 6.1 Medic VE-2023-47144  A flaw was found in Shim when an error happened while creating a			, , , , , , , , , , , , , , , , , , , ,			
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 QTS 4.5.4.2627 build 20231225 and later 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.  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: 2024-02-02 6.1 Medic VE-2023-47144  A flaw was found in Shim when an error happened while creating a	CVE-2023-38019		· · · · · · · · · · · · · · · · · · ·	2024-02-02	6.5	Mediun
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  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.  1BM 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: 2024-02-02 6.1 Medic A flaw was found in Shim when an error happened while creating a			An incorrect authorization vulnerability has been reported to			
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  BM 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.  BM 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 tivoli_application_d ependency_discove ry_manager  CVE-2023-47144  CVE-2023-47144  A flaw was found in Shim when an error happened while creating a			, , , , , , , , , , , , , , , , , , , ,			
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  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.  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: 2024-02-02 6.1 Medic CVE-2023-47144  A flaw was found in Shim when an error happened while creating a			,			
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  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.  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: 2024-02-02 6.1 Medic CVE-2023-47144  A flaw was found in Shim when an error happened while creating a						
qnap - multiple products QTS 4.5.4.2627 build 20231225 and later QTS 4.5.4.2627 build 20231225 and later  UBM 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.  UBM 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.  A flaw was found in Shim when an error happened while creating a			Q15 5.x, Qu15 nero are not affected.			
qnap - multiple products QTS 4.5.4.2627 build 20231225 and later QTS 4.5.4.2627 build 20231225 and later  UBM 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.  UBM 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.  A flaw was found in Shim when an error happened while creating a			We have already fixed the vulnerability in the following versions:			
CVE-2023-32967 products QTS 4.5.4.2627 build 20231225 and later 2024-02-02 6.5 Media 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 Media 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: 2024-02-02 6.1 Media Power Script Script Script IBM X-Force ID: 270271. 2024-02-02 6.1 Media A flaw was found in Shim when an error happened while creating a		gnap - multiple				
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 Medic 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 tivoli_application_d ependency_discove to credentials disclosure within a trusted session. IBM X-Force ID: 2024-02-02 6.1 Medic IBM X-Force ID: 275113. 2024-02-02 6.1 Medic IBM X-Force ID	CVE-2023-32967			2024-02-02	6.5	Mediun
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.  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: 2024-02-02 6.1 Medic CVE-2023-47144    A flaw was found in Shim when an error happened while creating a		,				
products  security context of the hosting site. IBM X-Force ID: 275113.  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:  2024-02-02  6.1 Medic  Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID:  A flaw was found in Shim when an error happened while creating a			•			
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 ependency_discove ry_manager  270271. A flaw was found in Shim when an error happened while creating a		•				
through 7.3.0.10 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the tivoli_application_d ependency_discove ry_manager  EVE-2023-47144  A flaw was found in Shim when an error happened while creating a  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: 2024-02-02  A flaw was found in Shim when an error happened while creating a		products	·	2024-02-02	6.1	Mediun
ibm - tivoli_application_d ependency_discove ry_manager  Z70271.  A flaw was found in Shim when an error happened while creating a  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:  2024-02-02  6.1 Mediu	CVE-2023-50933		,, , , , , , , , , , , , , , , , , , , ,			
tivoli_application_d ependency_discove ry_manager 270271. Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 2024-02-02 6.1 Media A flaw was found in Shim when an error happened while creating a	CVE-2023-50933		, ,			
ependency_discove to credentials disclosure within a trusted session. IBM X-Force ID:  ry_manager 270271. 2024-02-02 6.1 Mediu  A flaw was found in Shim when an error happened while creating a	CVE-2023-50933	ihm	i vumerability allows users to embed arbitrary JavaScript code in the	1		
CVE-2023-47144 ry_manager 270271. 2024-02-02 6.1 Media A flaw was found in Shim when an error happened while creating a	CVE-2023-50933		Web III thus altering the intended functionality notantially leading			
A flaw was found in Shim when an error happened while creating a	CVE-2023-50933	tivoli_application_d	, , ,			
		tivoli_application_d ependency_discove	to credentials disclosure within a trusted session. IBM X-Force ID:	2024-02-02	6.1	Mediun
new test variables it shift fails to steate the flew variable, it tites to		tivoli_application_d ependency_discove	to credentials disclosure within a trusted session. IBM X-Force ID: 270271.	2024-02-02	6.1	Medium

		parameters used by the logging function doesn't match the format			
		string used by it, leading to a crash under certain circumstances.			
		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			
CVE 2022 40E40	redhat - shim	flaw allows an attacker to load a crafted PE binary, triggering the	2024 01 20		Modium
CVE-2023-40549	reanat - snim	issue and crashing Shim, resulting in a denial of service.  An out-of-bounds read flaw was found in Shim when it tried to	2024-01-29	5.5	Medium
		validate the SBAT information. This issue may expose sensitive			
CVE-2023-40550	redhat - shim	data during the system's boot phase.	2024-01-29	5.5	Medium
<u> </u>	Teanac Siliii	In Spring Cloud Contract, versions 4.1.x prior to 4.1.1, versions	20210123	3.3	meanan
		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.			
CVE 2024 2222C	vmware - multiple		2024 04 24		Na sali sa
CVE-2024-22236	products		2024-01-31	5.5	Medium
		Dall Dawerscale Oness versions 9.2 v through 0.6.0 v centains an			
		Dell PowerScale OneFS versions 8.2.x through 9.6.0.x contains an incorrect default permissions vulnerability. A local low privileges			
	dell -	malicious user could potentially exploit this vulnerability, leading			
CVE-2024-22430	powerscale_onefs	to denial of service.	2024-02-01	5.5	Medium
<u>CVL 2024 22430</u>	powerscare_oners	IBM Security Access Manager Container (IBM Security Verify	2024 02 01	3.3	ivicaian
		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			
	ibm - multiple	download files from an incorrect repository due to improper file			
CVE-2023-32329	products	validation. IBM X-Force ID: 254972.	2024-02-03	5.5	Medium
	•	IBM PowerSC 1.3, 2.0, and 2.1 does not provide logout			
		functionality, which could allow an authenticated user to gain			
	ibm - multiple	access to an unauthorized user using session fixation. IBM X-Force			
CVE-2023-50941	products	ID: 275131.	2024-02-02	5.4	Mediun
		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			
	ibm -	functionality potentially leading to credentials disclosure within a			
CVE-2022-40744	aspera_faspex	trusted session. IBM X-Force ID: 236441.	2024-02-02	5.4	Medium
		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			
	ماسنطان مصنوع	section. This allows any authenticated user to execute arbitrary			
CVE-2023-51072	nagios - multiple products	JavaScript code on behalf of other users, including the administrators.	2024-02-02	5.4	Medium
CVE-2023-31072	products	A cross-site scripting (XSS) vulnerability has been reported to	2024-02-02	3.4	Medium
		affect Photo Station. If exploited, the vulnerability could allow			
		authenticated users to inject malicious code via a network.			
	qnap -	We have already fixed the vulnerability in the following version:			
CVE-2023-47561	photo_station	Photo Station 6.4.2 ( 2023/12/15 ) and later	2024-02-02	5.4	Medium
		IBM PowerSC 1.3, 2.0, and 2.1 uses insecure HTTP methods which			
	ibm - multiple	could allow a remote attacker to perform unauthorized file			
CVE-2023-50327	products	request modification. IBM X-Force ID: 275109.	2024-02-02	5.3	Medium
		IBM PowerSC 1.3, 2.0, and 2.1 may allow a remote attacker to			
	ibm - multiple	view session identifiers passed via URL query strings. IBM X-Force			
CVE-2023-50328	products	ID: 275110.	2024-02-02	5.3	Medium
		IBM PowerSC 1.3, 2.0, and 2.1 uses single-factor authentication			
		which can lead to unnecessary risk of compromise when compared			
	ibm - multiple	with the benefits of a dual-factor authentication scheme. IBM X-			
CVE-2023-50934	products	Force ID: 275114.	2024-02-02	5.3	Medium
		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 fellowing versions			
		We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later			
	gnap - multiple	Q15 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later			
CVE-2023-41274	products	QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	Medium
O V L 2023-412/4	products	A path traversal vulnerability has been reported to affect several	202 <del>1</del> -02-02	7.3	iviculull
		QNAP operating system versions. If exploited, the vulnerability			
		could allow authenticated administrators to read the contents of			
I I		unexpected files and expose sensitive data via a network.			
		Turicxpected files and expose sensitive data via a nerwork.			
		diexpected files and expose sensitive data via a fietwork.			
	qnap - multiple	We have already fixed the vulnerability in the following versions:			

		QuTS hero h5.1.5.2647 build 20240118 and later			
		QuTScloud c5.1.5.2651 and later			
		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			
	gnap - multiple	QuTS hero h5.1.5.2647 build 20240118 and later			
CVE-2023-45027	products	QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	Medium
<u> </u>	products	An uncontrolled resource consumption vulnerability has been	20210202	5	Mediam
		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.			
		The state of the s			
		We have already fixed the vulnerability in the following versions:			
		QTS 5.1.5.2645 build 20240116 and later			
	gnap - multiple	QuTS hero h5.1.5.2647 build 20240118 and later			
CVE-2023-45028	products	QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	Medium
	'	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			
	ibm - multiple	vulnerability to hijack the victim's click actions and possibly launch			
CVE-2023-50938	products	further attacks against the victim. IBM X-Force ID: 275128.	2024-02-02	4.3	Medium
	ibm -	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an			
	soar_qradar_plugin	authenticated user to manipulate output written to log files. IBM			
CVE-2023-38020	_app	X-Force ID: 260576.	2024-02-02	4.3	Medium

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