

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 للتُغرات 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 16th را يوليو إلى National Vulnerability Database (NVD) of July to 22nd of July. Vulnerabilities are scored using the Common معيار معيار معيار of July to 22nd of July. Vulnerabilities are scored using the Common يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Vulnerability Scoring System (CVSS) standard as per the following حيث يتم تصنيف الثغرات بناء على Vulnerability Scoring System (CVSS) 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

التالي:

عالى جدًا: النتيجة الأساسية لـ10.0-CVSS 9.0

عالى: النتيجة الأساسية لـ8.9-7.0 CVSS

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
		CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V1.8.0 on windows\linux\mac os e.g. platforms			
		allows attackers to send controlled message and			
		remote code execute via rabbitmq messages. Users can use the			
CVE 2022 20542	apache -	code under the master branch in project repo to fix this issue, we	2022 07 47	0.0	Cuiti a a l
CVE-2023-26512	eventmesh	will release the new version as soon as possible. An issue was discovered in the Linux kernel before 6.3.8.	2023-07-17	9.8	Critical
		fs/smb/server/smb2pdu.c in ksmbd has an integer underflow and			
CVE-2023-38427	linux - linux_kernel	out-of-bounds read in deassemble_neg_contexts.	2023-07-18	9.8	Critical
	_	An issue was discovered in the Linux kernel before 6.3.4.			
		fs/ksmbd/connection.c in ksmbd has an off-by-one error in			
		memory allocation (because of ksmbd_smb2_check_message)			
CVE-2023-38429	linux - linux_kernel	that may lead to out-of-bounds access.	2023-07-18	9.8	Critical
		Using "**" as a pattern in Spring Security configuration			
		for WebFlux creates a mismatch in pattern matching between			
	vmware - multiple	Spring Security and Spring WebFlux, and the potential for a security			
CVE-2023-34034	products	bypass.	2023-07-19	9.8	Critical
<u> </u>	citrix - multiple	Sypuss.	2023 07 13	3.0	Circical
CVE-2023-3519	products	Unauthenticated remote code execution	2023-07-19	9.8	Critical
	,	Out-of-bounds write when handling split HTTP headers; When			
		handling split HTTP headers, GRUB2 HTTP code accidentally moves			
		its internal data buffer point by one position. This can lead to a			
		out-of-bound write further when parsing the HTTP request, writing			
		a NULL byte past the buffer. It's conceivable that an attacker			
CVE 2022 20724		controlled set of packets can lead to corruption of the GRUB2's	2022 07 20	0.0	Cuitinal
CVE-2022-28734	gnu - grub2	internal memory metadata.	2023-07-20	9.8	Critical
		Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization			
		of Untrusted Data vulnerability that could result in Arbitrary code			
	adobe - multiple	execution. Exploitation of this issue does not require user			
CVE-2023-38203	products	interaction.	2023-07-20	9.8	Critical
	,	An issue was discovered in the Linux kernel before 6.3.4. ksmbd			
		has an out-of-bounds read in smb2_find_context_vals when			
CVE-2023-38426	linux - linux_kernel	create_context's name_len is larger than the tag length.	2023-07-18	9.1	Critical
		An issue was discovered in the Linux kernel before 6.3.4.			
		fs/ksmbd/smb2pdu.c in ksmbd does not properly check the			
CVE 2022 20420	linux linux kornal	UserName value because it does not consider the address of	2022 07 10	0.1	Critical
CVE-2023-38428	linux - linux_kernel	security buffer, leading to an out-of-bounds read. An issue was discovered in the Linux kernel before 6.3.9. ksmbd	2023-07-18	9.1	Critical
		does not validate the SMB request protocol ID, leading to an out-			
CVE-2023-38430	linux - linux_kernel	of-bounds read.	2023-07-18	9.1	Critical
		An issue was discovered in the Linux kernel before 6.3.8.			
		fs/smb/server/connection.c in ksmbd does not validate the			
CVE-2023-38431	linux - linux_kernel	relationship between the NetBIOS header's length field and the	2023-07-18	9.1	Critical

		SMB header sizes, via pdu_size in ksmbd_conn_handler_loop,			
		leading to an out-of-bounds read. An issue was discovered in the Linux kernel before 6.3.10.			
		fs/smb/server/smb2misc.c in ksmbd does not validate the			
CVE-2023-38432	linux - linux kernel	relationship between the command payload size and the RFC1002 length specification, leading to an out-of-bounds read.	2023-07-18	9.1	Critica
CVL-2023-38432	iiiidx - iiiidx_kerriei	Vulnerability in the Application Express Team Calendar Plugin	2023-07-18	J.1	Critica
		product of Oracle Application Express (component: User Account).			
		Supported versions that are affected are Application Express Team			
		Calendar Plugin: 18.2-22.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to			
		compromise Application Express Team Calendar Plugin. Successful			
		attacks require human interaction from a person other than the			
		attacker and while the vulnerability is in Application Express Team Calendar Plugin, attacks may significantly impact additional			
		products (scope change). Successful attacks of this vulnerability			
		can result in takeover of Application Express Team Calendar			
	oracle -	Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
CVE-2023-21974	application_express	(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	2023-07-18	9	Critica
		Vulnerability in the Application Express Customers Plugin product			
		of Oracle Application Express (component: User Account).			
		Supported versions that are affected are Application Express Customers Plugin: 18.2-22.2. Easily exploitable vulnerability allows			
		low privileged attacker with network access via HTTP to			
		compromise Application Express Customers Plugin. Successful			
		attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express			
		Customers Plugin, attacks may significantly impact additional			
		products (scope change). Successful attacks of this vulnerability			
		can result in takeover of Application Express Customers Plugin.			
	oracle -	CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
CVE-2023-21975	application_express	, ,	2023-07-18	9	Critica
		The configuration parser fails to sanitize user-controlled input in			
		the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W)			
		series firmware versions 5.10 through 5.36,			
		-			
		USG20(W)-VPN series firmware versions 5.10 through 5.36, and			
		VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the			
		vulnerability to inject some operating system (OS) commands into			
	zyxel - usg_2200-	the device configuration data on an affected device when the			
CVE-2023-28767	vpn_firmware	cloud management mode is enabled. A format string vulnerability in the Zyxel ATP series firmware	2023-07-17	8.8	High
		versions 5.10 through 5.36 Patch 2, USG FLEX series firmware			
		versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series			
		firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series			
		firmware versions 5.00 through 5.36 Patch 2, could allow an			
		unauthenticated, LAN-based attacker to execute some OS			
CVE 2022 22011	zyxel - usg_2200-	commands by using a crafted PPPoE configuration on an affected	2022 07 17	0.0	ماء: ١١: ﻣﺎﻣ
CVE-2023-33011	vpn_firmware	device when the cloud management mode is enabled. A command injection vulnerability in the configuration parser of	2023-07-17	8.8	High
		the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2,			
		USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG			
		FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch			
		2, and VPN series firmware versions 5.00 through 5.36 Patch			
		2, could allow an unauthenticated, LAN-based attacker to execute			
CVE_2022 22012	zyxel - usg_20w- vpn firmware	some OS commands by using a crafted GRE configuration when	2023-07-17	8.8	امہ;∟
CVE-2023-33012	vhii_iiiIiiwate	the cloud management mode is enabled. A command injection vulnerability in the Free Time WiFi hotspot	2023-07-17	0.0	High
		feature of the Zyxel USG FLEX series firmware versions 4.50			
		through 5.36 Patch 2 and VPN series firmware versions 4.20			
CVE-2023-34139	zyxel - usg_2200- vpn firmware	through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device.	2023-07-17	8.8	High
CAT 7072-24122	vpii_iiiiiwaie	The XPRTLD web application in Veritas InfoScale Operations	∠ULJ-U/-1/	0.0	ıııgıı
		Manager (VIOM) before 8.0.0.410 allows an authenticated			
	veritas -	attacker to upload all types of files to the server. An authenticated			
CVE-2023-38404	infoscale_operation s_manager	attacker can then execute the malicious file to perform command execution on the remote server.	2023-07-17	8.8	High
	5565.	Deserialization of Untrusted Data vulnerability in Apache			6.1
		ShardingSphere-Agent, which allows attackers to execute arbitrary			
		code by constructing a special YAML configuration file.			
		The attacker needs to have permission to modify the			
		· · · · · · · · · · · · · · · · · · ·			
CVE-2023-28754	apache - shardingsphere	ShardingSphere Agent YAML configuration file on the target machine, and the target machine can access the URL with the	2023-07-19	8.8	High

		T 100			
		arbitrary code JAR. An attacker can use SnakeYAML to deserialize			
		java.net.URLClassLoader and make it load a JAR from a specified			
		URL, and then deserialize javax.script.ScriptEngineManager to load			
		code using that ClassLoader. When the ShardingSphere JVM			
		process starts and uses the ShardingSphere-Agent, the arbitrary			
		code specified by the attacker will be executed during the deserialization of the YAML configuration file by the Agent.			
		desertalization of the PAIVIL configuration file by the Agent.			
		This issue affects ShardingSphere-Agent: through 5.3.2. This			
		vulnerability is fixed in Apache ShardingSphere 5.4.0.			
		Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version			
		that is affected is 11.2.13.0.000. Easily exploitable vulnerability			
		allows low privileged attacker with network access via HTTP to			
		compromise Oracle Hyperion Financial Reporting. While the			
		vulnerability is in Oracle Hyperion Financial Reporting, attacks may			
		significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to			
		critical data or complete access to all Oracle Hyperion Financial			
		Reporting accessible data and unauthorized ability to cause a			
		partial denial of service (partial DOS) of Oracle Hyperion Financial			
		Reporting. CVSS 3.1 Base Score 8.5 (Confidentiality and Availability			
CVE 2022 220C2	oracla burarian	impacts). CVSS Vector:	2022 07 40	0 -	11:
CVE-2023-22062	oracle - hyperion	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L). Vulnerability in the PeopleSoft Enterprise PeopleTools product of	2023-07-18	8.5	High
		Oracle PeopleSoft (component: Portal). Supported versions that			
		are affected are 8.59 and 8.60. Easily exploitable vulnerability			
		allows unauthenticated attacker with logon to the infrastructure			
		where PeopleSoft Enterprise PeopleTools executes to compromise			
		PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise			
		PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and			
	oracle - multiple	Availability impacts). CVSS Vector:			
CVE-2023-22014	products	(CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-07-18	8.4	High
		Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are			
		affected are Prior to 6.1.46 and Prior to 7.0.10. Difficult to exploit			
		vulnerability allows unauthenticated attacker with network access			
		via RDP to compromise Oracle VM VirtualBox. Successful attacks			
		of this vulnerability can result in takeover of Oracle VM VirtualBox.			
	oracle - multiple	CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
CVE-2023-22018	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-07-18	8.1	High
		Integer underflow in grub_net_recv_ip4_packets; A malicious			
		crafted IP packet can lead to an integer underflow in			
		grub_net_recv_ip4_packets() function on rsm->total_len value. Under certain circumstances the total_len value may end up			
		wrapping around to a small integer number which will be used in			
		memory allocation. If the attack succeeds in such way, subsequent			
CVE-2022-28733	gnu - grub2	operations can write past the end of the buffer.	2023-07-20	8.1	High
		A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through			
		5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36			
		Patch 2, USG FLEX 50(W) series firmware versions 4.60 through			
		5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60			
		through 5.36 Patch 2, and VPN series firmware versions 4.60			
		through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if			
	zyxel - usg_20w-	the attacker could trick an authorized administrator to add their IP			
CVE-2023-34138	vpn_firmware	address to the list of trusted RADIUS clients in advance.	2023-07-17	8	High
		A command injection vulnerability in the access point (AP)			
		management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00			
		through 5.36 Patch 2, USG FLEX 50(W) series firmware versions			
		5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware			
		versions 5.00 through 5.36 Patch 2, VPN series firmware versions			
		5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware			
		versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an			
		unauthenticated, LAN-based attacker to execute some OS			
		commands on an affected device if the attacker could trick an			
CVE 2022 244.44	zyxel - usg_20w-	authorized administrator to add their IP address to the managed	2022 07 47	c	مانية (1
CVE-2023-34141	vpn_firmware citrix - multiple	AP list in advance.	2023-07-17	8	High
CVE-2023-3467	products	Privilege Escalation to root administrator (nsroot)	2023-07-19	8	High
		The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i			-
CVE 2022 20000	ibm - multiple	contains a local privilege escalation vulnerability. A malicious	2022 07 40	7.0	ماند (۱
CVE-2023-30988	products	actor with command line access to the host operating system can	2023-07-16	7.8	High

		elevate privileges to gain root access to the host operating system. IBM X-Force ID: 254016.			
		IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local			
		privilege escalation vulnerability. A malicious actor with command			
		line access to the host operating system can elevate privileges to			
	ibm - multiple	gain all object access to the host operating system. IBM X-Force			
CVE-2023-30989	products	ID: 254017.	2023-07-16	7.8	High
		Vulnerability in the Oracle Solaris product of Oracle Systems			
		(component: Device Driver Interface). The supported version that			
		is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle			
		Solaris executes to compromise Oracle Solaris. Successful attacks			
		of this vulnerability can result in takeover of Oracle Solaris. Note:			
		CVE-2023-22023 is equivalent to CVE-2023-31284. CVSS 3.1 Base			
		Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS			
CVE-2023-22023	oracle - solaris	Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2023-07-18	7.8	High
	:1	IBM Security Guardium 11.3 could allow a local user to escalate			
CVE-2022-43910	ibm -	their privileges due to improper permission controls. IBM X-Force ID: 240908.	2023-07-19	7.8	⊔iah
CVE-2022-45910	security_guardium	The GRUB2's shim_lock verifier allows non-kernel files to be	2023-07-19	7.0	High
		loaded on shim-powered secure boot systems. Allowing such files			
		to be loaded may lead to unverified code and modules to be			
CVE-2022-28735	gnu - grub2	loaded in GRUB2 breaking the secure boot trust-chain.	2023-07-20	7.8	High
		There's a use-after-free vulnerability in grub_cmd_chainloader()			
		function; The chainloader command is used to boot up operating			
		systems that doesn't support multiboot and do not have direct			
		support from GRUB2. When executing chainloader more than			
		once a use-after-free vulnerability is triggered. If an attacker can control the GRUB2's memory allocation pattern sensitive data may			
CVE-2022-28736	gnu - grub2	be exposed and arbitrary code execution can be achieved.	2023-07-20	7.8	High
<u>CVL 2022 20730</u>	giia giabz	There's a possible overflow in handle_image() when shim tries to	2023 07 20	7.0	111611
		load and execute crafted EFI executables; The handle_image()			
		function takes into account the SizeOfRawData field from each			
		section to be loaded. An attacker can leverage this to perform out-			
		of-bound writes into memory. Arbitrary code execution is not			
CVE-2022-28737	redhat - shim	discarded in such scenario.	2023-07-20	7.8	High
		Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier)			
		are affected by an out-of-bounds write vulnerability that could			
		result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			
CVE-2021-39822	adobe - indesign	victim must open a malicious BMP file.	2023-07-20	7.8	High
<u> </u>	adobe maesign	Vulnerability in the Oracle Hyperion Workspace product of Oracle	2023 07 20	7.0	6
		Hyperion (component: UI and Visualization). The supported			
		version that is affected is 11.2.13.0.000. Easily exploitable			
		vulnerability allows low privileged attacker with network access via			
		HTTP to compromise Oracle Hyperion Workspace. Successful			
		attacks require human interaction from a person other than the			
		attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical			
		data or all Oracle Hyperion Workspace accessible data as well as			
		unauthorized access to critical data or complete access to all			
		Oracle Hyperion Workspace accessible data and unauthorized			
		ability to cause a partial denial of service (partial DOS) of Oracle			
	oracle -	Hyperion Workspace. CVSS 3.1 Base Score 7.6 (Confidentiality,			
	hyperion_workspac	Integrity and Availability impacts). CVSS Vector:			
CVE-2023-22060	е	(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L).	2023-07-18	7.6	High
		TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer			
	to link	C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_USV1_170228 were discovered to contain a buffer			
	tp-link - archer_c2_v1_firm	overflow which may lead to a Denial of Service (DoS) when parsing			
CVE-2023-30383	ware	crafted data.	2023-07-18	7.5	High
212 2020 00000	7.4.0	Vulnerability in the PeopleSoft Enterprise PeopleTools product of			6''
		Oracle PeopleSoft (component: Portal). Supported versions that			
		are affected are 8.59 and 8.60. Easily exploitable vulnerability			
		allows unauthenticated attacker with network access via HTTP to			
		compromise PeopleSoft Enterprise PeopleTools. Successful			
		attacks of this vulnerability can result in unauthorized access to			
Į.		critical data or complete access to all PeopleSoft Enterprise			
		• • • • • • • • • • • • • • • • • • • •			
	oracle - multiple	PeopleTools accessible data. CVSS 3.1 Base Score 7.5			
CVF-2023-22047	oracle - multiple products	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector:	2023-07-18	7.5	High
CVE-2023-22047	oracle - multiple products	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	7.5	High
CVE-2023-22047	•	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector:	2023-07-18	7.5	High
CVE-2023-22047 CVE-2021-38933	products	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). IBM Sterling Connect:Direct for UNIX 1.5 uses weaker than	2023-07-18	7.5 7.5	High High
	products ibm -	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). IBM Sterling Connect:Direct for UNIX 1.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210574. Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes			_
	ibm - sterling_connect\ ibm -	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). IBM Sterling Connect:Direct for UNIX 1.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210574. Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to			_
	ibm - sterling_connect\	PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). IBM Sterling Connect:Direct for UNIX 1.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210574. Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes			_

		Planning Applytics Contribute for Clark St. D. 1. C.			
	ibm -	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to			
	cloud_pak_for_dat	exploit this vulnerability to conduct further attacks. IBM X-Force			
CVE-2023-26026	a	ID: 247896.	2023-07-19	7.5	High
		IBM Planning Analytics Cartridge for Cloud Pak for Data 4.0			
	ibm -	connects to a CouchDB server. An attacker can exploit an insecure			
	cloud_pak_for_dat	password policy to the CouchDB server and collect sensitive			
CVE-2023-27877	a	information from the database. IBM X-Force ID: 247905.	2023-07-19	7.5	High
		An out-of-bounds read vulnerability was found in Samba due to			
		insufficient length checks in winbindd_pam_auth_crap.c. When			
		performing NTLM authentication, the client replies to cryptographic challenges back to the server. These replies have			
		variable lengths, and Winbind fails to check the lan manager			
		response length. When Winbind is used for NTLM authentication,			
	samba - multiple	a maliciously crafted request can trigger an out-of-bounds read in			
CVE-2022-2127	products	Winbind, possibly resulting in a crash.	2023-07-20	7.5	High
		MikroTik RouterOS stable before 6.49.7 and long-term through			
		6.48.6 are vulnerable to a privilege escalation issue. A remote and			
	مامنطاريمس بانجمسانيمس	authenticated attacker can escalate privileges from admin to			
CVE-2023-30799	mikrotik - multiple products	super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system.	2023-07-19	7.2	High
CVL-2023-30799	products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect	2023-07-13	1.2	High
		Server) 11.5 with a Federated configuration is vulnerable to a			
		stack-based buffer overflow, caused by improper bounds checking.			
		A local user with SYSADM privileges could overflow the buffer and			
CVE-2023-35012	ibm - db2	execute arbitrary code on the system. IBM X-Force ID: 257763.	2023-07-17	6.7	Medium
		A buffer copy without checking size of input ('classic buffer			
		overflow') in Fortinet FortiAnalyzer version 7.0.2 and below,			
		version 6.4.7 and below, version 6.2.9 and below, version 6.0.11			
		and below, version 5.6.11 and below, FortiManager version 7.0.2 and below, version 6.4.7 and below, version 6.2.9 and below,			
		version 6.0.11 and below, version 5.6.11 and below, FortiOS			
		version 7.0.0 through 7.0.4, 6.4.0 through 6.4.8, 6.2.0 through			
		6.2.10, 6.0.x and FortiProxy version 7.0.0 through 7.0.3, 2.0.0			
		through 2.0.8, 1.2.x, 1.1.x and 1.0.x allows attacker to execute			
		unauthorized code or commands via crafted CLI `execute restore			
	fortinet - multiple	image` and `execute certificate remote` operations with the tFTP			
CVE-2021-43072	products	protocol.	2023-07-18	6.7	Medium
		A buffer overflow vulnerability in the Zyxel ATP series firmware			
		versions 4.32 through 5.36 Patch 2, USG FLEX series firmware			
		versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN			
		series firmware versions 4.16 through 5.36 Patch 2, VPN series			
		firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware			
		versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500			
		firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow			
		an unauthenticated, LAN-based attacker to cause denial of service			
	zyxel - usg_20w-	(DoS) conditions by sending a crafted request to the CAPWAP			
CVE-2023-34140	zyxel - usg_20w- vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon.	2023-07-17	6.5	Medium
CVE-2023-34140		(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU	2023-07-17	6.5	Medium
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-			
CVE-2023-34140 CVE-2021-32256		(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	2023-07-17	6.5	
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle			
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.			
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator			
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to			
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to			
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of			
	vpn_firmware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data			
	vpn_firmware gnu - binutils	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible			
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS	2023-07-18	6.5	Medium
	vpn_firmware gnu - binutils	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or	2023-07-18	6.5	Medium
CVE-2021-32256	vpn_firmware gnu - binutils oracle -	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data	2023-07-18	6.5	Medium
CVE-2021-32256	oracle - fusion_middleware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5	2023-07-18	6.5	Medium
CVE-2021-32256 CVE-2023-21994	oracle - fusion_middleware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector:	2023-07-18	6.5	Medium
CVE-2021-32256	oracle - fusion_middleware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle_c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite accessful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium Medium
CVE-2021-32256 CVE-2023-21994	oracle - fusion_middleware oracle - products	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle_c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium
CVE-2021-32256 CVE-2023-21994	oracle - fusion_middleware	(DoS) conditions by sending a crafted request to the CAPWAP daemon. An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle_c. Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite accessful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium

					•
		network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access			
		via multiple protocols to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and			
CVE-2023-22040	oracle - multiple products ibm - infosphere_informa	Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer.	2023-07-18	6.5	Medium
CVE-2023-35898	tion_server	IBM X-Force ID: 259352.	2023-07-19	6.5	Medium
CVE-2022-43908	ibm - security_guardium	IBM Security Guardium 11.3 could allow an authenticated user to cause a denial of service due to improper input validation. IBM X-Force ID: 240903.	2023-07-19	6.5	Medium
		A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/			
CVE 2022 22264	microfocus -		2022 07 40	6.5	D. A. a. diaman
CVE-2023-32261	dimensions_cm	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Item/Configure permission to access and capture credentials they are not entitled to. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/	2023-07-19	6.5	Medium
CVE-2023-32262	microfocus - dimensions_cm		2023-07-19	6.5	Medium
CVE-2023-32481	dell - wyse_management suite	Wyse Management Suite versions prior to 4.0 contain a denial-of-service vulnerability. An authenticated malicious user can flood the configured SMTP server with numerous requests in order to deny access to the system.	2023-07-20	6.5	Medium
	solarwinds - database_performa	XSS attack was possible in DPA 2023.2 due to insufficient input			
CVE-2023-33231 CVE-2023-22035	oracle - e- business_suite	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: iSurvey Module). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-07-18	6.1	Medium
CVE-2023-22035	pusiness_suite	(CV33.3.1/AV.IV/AC.L/FN.IV/UI.N/3.C/C.L/T.L/A.IV).	ZUZ3-U/-18	0.1	ivieululii

	T				1
		Vulnerability in the Oracle Applications Framework product of			
		Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.3-12.3.12. Easily exploitable			
		vulnerability allows unauthenticated attacker with network access			
		via HTTP to compromise Oracle Applications Framework.			
		Successful attacks require human interaction from a person other			
		than the attacker and while the vulnerability is in Oracle			
		Applications Framework, attacks may significantly impact			
		additional products (scope change). Successful attacks of this			
		vulnerability can result in unauthorized update, insert or delete			
		access to some of Oracle Applications Framework accessible data			
		as well as unauthorized read access to a subset of Oracle			
	oracle -	Applications Framework accessible data. CVSS 3.1 Base Score 6.1			
	applications_frame	(Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22042	work	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-07-18	6.1	Medium
		Vulnerability in the JD Edwards EnterpriseOne Tools product of			
		Oracle JD Edwards (component: Web Runtime SEC). Supported			
		versions that are affected are Prior to 9.2.7.4. Easily exploitable			
		vulnerability allows unauthenticated attacker with network access			
		via HTTP to compromise JD Edwards EnterpriseOne Tools.			
		Successful attacks require human interaction from a person other			
		than the attacker and while the vulnerability is in JD Edwards			
		EnterpriseOne Tools, attacks may significantly impact additional			
		products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some			
		of JD Edwards EnterpriseOne Tools accessible data as well as			
		unauthorized read access to a subset of JD Edwards EnterpriseOne			
	oracle -	Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and			
	jd_edwards_enterp	Integrity impacts). CVSS Vector:			
CVE-2023-22055	riseone_tools	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-07-18	6.1	Medium
	citrix - multiple	, , , , , , , , , , , , , , , , , , , ,		-	2 2.7 4.111
CVE-2023-3466	products	Reflected Cross-Site Scripting (XSS)	2023-07-19	6.1	Medium
		Vulnerability in the Oracle Hyperion Essbase Administration			
		Services product of Oracle Essbase (component: EAS			
		Administration and EAS Console). The supported version that is			
		affected is 21.4.3.0.0. Easily exploitable vulnerability allows high			
		privileged attacker with logon to the infrastructure where Oracle			
		Hyperion Essbase Administration Services executes to compromise			
		Oracle Hyperion Essbase Administration Services. While the			
		vulnerability is in Oracle Hyperion Essbase Administration Services,			
		attacks may significantly impact additional products (scope			
		change). Successful attacks of this vulnerability can result in			
	oracle -	unauthorized access to critical data or complete access to all			
	hyperion_essbase_	Oracle Hyperion Essbase Administration Services accessible data.			
015 0000 5155	administration_ser	CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector:	2022 2=	_	
CVE-2023-21961	vices	(CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2023-07-18	6	Medium
		Vulnerability in Oracle Java SE (component: JavaFX). The			
		supported version that is affected is Oracle Java SE: 8u371.			
		Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle			
		Java SE. Successful attacks of this vulnerability can result in			
		unauthorized creation, deletion or modification access to critical			
		data or all Oracle Java SE accessible data. Note: This vulnerability			
		applies to Java deployments, typically in clients running sandboxed			
		Java Web Start applications or sandboxed Java applets, that load			
		and run untrusted code (e.g., code that comes from the internet)			
		and rely on the Java sandbox for security. This vulnerability does			
		not apply to Java deployments, typically in servers, that load and			
		run only trusted code (e.g., code installed by an administrator).			
	oracle - multiple	CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector:			
CVE-2023-22043	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	2023-07-18	5.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Client programs). Supported versions that are			
		affected are 5.7.42 and prior and 8.0.33 and prior. Difficult to			
		exploit vulnerability allows low privileged attacker with network			
		access via multiple protocols to compromise MySQL Server.			
		Successful attacks of this vulnerability can result in unauthorized			
		ability to cause a hang or frequently repeatable crash (complete			
		DOS) of MySQL Server and unauthorized read access to a subset			
		of MySQL Server accessible data. CVSS 3.1 Base Score 5.9			
	oracle - multiple	(Confidentiality and Availability impacts). CVSS Vector:	2022 27 12	- ^	N 4 11
0) /5 0000 0000				- C	Medium
CVE-2023-22053	products	(CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H).	2023-07-18	5.9	
CVE-2023-22053			2023-07-18	5.9	
CVE-2023-22053		A potential vulnerability has been identified in the Micro Focus	2023-07-18	5.9	
CVE-2023-22053		A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be	2023-07-18	5.9	
CVE-2023-22053		A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is	2023-07-18	5.9	
CVE-2023-22053		A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is duped into using an attacker-controlled Dimensions CM server.	2023-07-18	5.9	
<u>CVE-2023-22053</u>	products	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is duped into using an attacker-controlled Dimensions CM server. This vulnerability only applies when the Jenkins plugin is	2023-07-18	5.9	
CVE-2023-22053		A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is duped into using an attacker-controlled Dimensions CM server.	2023-07-18	5.7	Medium

		https://www.jenkins.io/security/advisory/2023-06-14/			
		Vulnerability in the Application Express Administration product of			
		Oracle Application Express (component: None). Supported			
		versions that are affected are Application Express Administration:			
		18.2-22.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Application			
		Express Administration. Successful attacks of this vulnerability can			
		result in unauthorized update, insert or delete access to some of			
		Application Express Administration accessible data as well as			
		unauthorized read access to a subset of Application Express			
		Administration accessible data and unauthorized ability to cause a			
		partial denial of service (partial DOS) of Application Express Administration. CVSS 3.1 Base Score 5.6 (Confidentiality, Integrity			
	oracle -	and Availability impacts). CVSS Vector:			
CVE-2023-21983	application_express	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).	2023-07-18	5.6	Medium
		An issue was discovered in set_con2fb_map in			
		drivers/video/fbdev/core/fbcon.c in the Linux kernel before			
		6.2.12. Because an assignment occurs only for the first vc, the fbcon_registered_fb and fbcon_display arrays can be			
		desynchronized in fbcon_mode_deleted (the con2fb_map points			
CVE-2023-38409	linux - linux kernel	at the old fb info).	2023-07-17	5.5	Medium
	_	A deadlock flaw was found in the Linux kernel's BPF subsystem.			
CVE-2023-0160	linux - linux_kernel	This flaw allows a local user to potentially crash the system.	2023-07-18	5.5	Medium
		ChakraCore branch master cbb9b was discovered to contain a			
CVE-2023-37139	microsoft - chakracore	stack overflow vulnerability via the function	2023-07-18	5.5	Medium
CVE-2U25-3/139	cnakracore	Js::ScopeSlots::IsDebuggerScopeSlotArray(). ChakraCore branch master cbb9b was discovered to contain a	2023-07-18	5.5	ivieulum
	microsoft -	segmentation violation via the function			
CVE-2023-37140	chakracore	Js::DiagScopeVariablesWalker::GetChildrenCount().	2023-07-18	5.5	Medium
		ChakraCore branch master cbb9b was discovered to contain a			
0.45 0000 05444	microsoft -	segmentation violation via the function			
CVE-2023-37141	chakracore	Js::ProfilingHelpers::ProfiledNewScArray(). ChakraCore branch master cbb9b was discovered to contain a	2023-07-18	5.5	Medium
	microsoft -	segmentation violation via the function			
CVE-2023-37142	chakracore	Js::EntryPointInfo::HasInlinees().	2023-07-18	5.5	Medium
	1,212	ChakraCore branch master cbb9b was discovered to contain a			
	microsoft -	segmentation violation via the function			
CVE-2023-37143	chakracore	BackwardPass::IsEmptyLoopAfterMemOp().	2023-07-18	5.5	Medium
		Vulnerability in the Oracle VM VirtualBox product of Oracle			
		Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable			
		vulnerability allows low privileged attacker with logon to the			
		infrastructure where Oracle VM VirtualBox executes to			
		compromise Oracle VM VirtualBox. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or			
		frequently repeatable crash (complete DOS) of Oracle VM			
	oracle - multiple	VirtualBox. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector:			
CVE-2023-22017	products	(CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	5.5	Medium
	,			-	
		Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a			
		sensitive information disclosure vulnerability. An unauthenticated			
CVE 2022 2244C	doll wwo things	malicious user with local access to the device could exploit this	2022 07 20		Madium
CVE-2023-32446	dell - wyse_thinos	vulnerability to read sensitive information written to the log files.	2023-07-20	5.5	Medium
		Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a			
		sensitive information disclosure vulnerability. A malicious user			
		with local access to the device could exploit this vulnerability to			
CVE-2023-32447	dell - wyse_thinos	read sensitive information written to the log files.	2023-07-20	5.5	Medium
		Doll Whise ThinOS versions prior to 2209 (0.2.2103) contains			
		Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated			
		malicious user with local access to the device could exploit this			
CVE-2023-32455	dell - wyse_thinos	vulnerability to read sensitive information written to the log files.	2023-07-20	5.5	Medium
		Vulnerability in the Oracle Business Intelligence Enterprise Edition			
		product of Oracle Analytics (component: Analytics Server).			
		Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0.			
		Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business			
		Intelligence Enterprise Edition. Successful attacks of this			
		vulnerability can result in unauthorized update, insert or delete			
		access to some of Oracle Business Intelligence Enterprise Edition			
		accessible data and unauthorized ability to cause a partial denial of			
		service (partial DOS) of Oracle Business Intelligence Enterprise			
	oracle - multiple	Edition. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector:			
CVE-2023-22011	products	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	2023-07-18	5.4	Medium
		, , , , , , , , , , , , , , , , , , , ,	= =		

product of Oracle Analytics (component Analytics Server). Supported verticals that are affected as e A LO D and 7 D D D. Eastly epiditable vulnerability allows fow privileged attacker with nativoris access that HTP to components Crale Business intelligence fertity and the components of the compone		<u> </u>	V 1 199 1 21 5 1 5 1 5 1 1 1 1 1 1 1 1 1 1 1 1		I	
Supported versions that are effected an 6.0.0.0 and 7.0.0.0. Easily exploitable vulnerability allow privaleged attacks of the voltage and the results of the voltage and voltage			Vulnerability in the Oracle Business Intelligence Enterprise Edition			
Easily exploitable vulnerability allows low privileged standors with network access with 11P to compromise Uracle business in melligence enterprise cition. Successful attacks of this vulnerability can result in unauthorate update, insent or delete access to some of Oracle submess trailingence Enterprise Edition. Control oracle supply control oracle business trailingence interprise Edition. Control oracle supply control oracle business trailingence interprise Edition accession to a Code Business trailingence for Enterprise Edition. Code Submess or Code Supply Code						
network access via HTTP to compromise Oracle business intelligence Enterprise Edition. Society of the control of the value access to some of oracle Supress. We represent the control of t			• •			
intelligence Enterprise Edition. Successful states of this vulnerability or a result in manuformed update, insent or delete access to some of Oracle subsenses intelligence Enterprise Edition accessible data cossible data was well as unsubtrated and access to a subset of Oracle & Business intelligence Enterprise Edition accessible data. CVS 3.1 Base Score 3.4 (Confidentially and Integry impact). Vollenzibility in the Oracle Agile PLM product of Oracle Supply Chain (component WebClent). The supported westion that is directed by 9.3.6 Easily exploitable underability allows low privileged attacker with network access via HTTP to componite Oracle Agile PLM. Successful attacks require human interaction from a person orber than the attacker and while the vulnerability is in Oracle Agile PLM. Successful attacks or require human interaction from a person orber than the attacker and while the vulnerability is in Oracle Agile PLM. Successful attacks or require human interaction from a person orber than the attacker and while the vulnerability is in Oracle Agile PLM. Successful attacks or the vulnerability is in Oracle Agile PLM. Successful attacks or require human interaction from a person orber of Oracle Agile PLM attacks between the vulnerability in the DE dwards (component E. LI IOT Context and Security). Supported versions that are affected are Prior to 9.2.7.4. Easily Agriculture orbital vulnerability in the ID Edwards Enterprise Oracle are Prior to 9.2.7.4. Easily Agriculture orbital vulnerability and v			, , ,			
volnerability can result in unauthorized update, insert or delice access to some of Oracle Business intelligence interrupts edition accessible data as well as unauthorized read access to a subset of Oracle Business intelligence interrupts in Edition accessible data (VSS 3.1 Base Score 8.4 (Confidentiality and integrity impacts). CVF-2073-72000 products Vulnerability in the Oracle again PLV product of Oracle supply CVF-2073-72000 products Vulnerability in the Oracle again PLV product of Oracle supply CVF-2073-72000 products Vulnerability in the Oracle again PLV product of Oracle supply CVF-2073-72000 products (VSS Veters). (VSS 1.1 keV products) and unauthorized update, interrection from a person other than the attacker and while the vulnerability is in Oracle Again PLM accessive data require human interrection from a person other than the attacker and while the vulnerability is in Oracle Again PLM accessive data as well as unauthorized access to one of Oracle Again PLM accessive data as well as unauthorized access to one of Oracle Again PLM accessive data as well as unauthorized access to one of Oracle Again PLM accessive data as well as unauthorized access to one of Oracle Again PLM accessive data as well as unauthorized access to oracle oracle again PLM accessive data as well as unauthorized access to oracle oracle again product of Oracle DE disvorts (components ELI) OF orthostrator security. Supported versions that are affected are print to 9.2.7.4. Fasily republished uninerability allows buy privileged attacker with network access will after the components of PLM accessive data accessive data accessive accessiv			· ·			
accessible data as well as unauthorized read accessible data cocssible data as well as unauthorized read accessible data accessible data as well as unauthorized read accessible data (VSS 3.1 lase score > 4.Conflicteritis) and integrity impacts). CVS 2023-22020 CVS 24 core (CVS 3.2 LARA/MACL/PREJ/UNIX/SU/CL/LIA/AN). Vollenchality in the Proteck page PM by moducal of Oracle Supply attented is 9.3 of. Easily exploitable various billy values billy values by attented is 9.3 of. Easily exploitable various billy values billy values by attented is 9.3 of. Easily exploitable various billy values billy values by a provided attacker of 9.3 of. Easily exploitable various billy values billy valu						
cve 2013-22020 products Cve 2013-22020 produc			·			
Oracle - multiple OVE-2023-2000 OVE			· · · · · · · · · · · · · · · · · · ·			
oracle - multiple CVS-33.1 Biose Score 5.4 (Confidentiality and Integrity Impacts). Vivinerability in the Oracle Agile PLM product of Oracle Supply Chain (component: WebClient). The supported versor to hat is affected is 9.3.6. Early exploitable vulnerability allows low privileged attacker with network access via HTTD to compromise Oracle Agile PLM. Successful attacks of the vulnerability is in Oracle Agile PLM. Successful attacks of the vulnerability is in Oracle Agile PLM. Successful attacks of the vulnerability is in Oracle Agile PLM. Successful attacks of the vulnerability is in Oracle Agile PLM. Successful attacks of the vulnerability can result in unauthorized update, isset or delete access to some access via a tract of the vulnerability is in Oracle Agile PLM. Attacks may significantly impacts additional products (Social Agile PLM accessive last acts of this vulnerability can result in unauthorized update, isset or delete access to some access via a tract of the vulnerability in the ID Edwards Enterprised Conforced Explaints (Social Agile PLM accessive last acts of the vulnerability in the ID Edwards Enterprised Conforced Explaints (Social Agile PLM accessive last acts of the vulnerability in the ID Edwards Enterprised Conforced Explaints (Social Agile PLM accessive last acts of the vulnerability in the ID Edwards Enterprised Conforced Explaints (Social Explaints) (Soci						
CVE-2023-22030 products CVSS Vector: (CVSS-31/AVN)ACL/PRIA/LIN/NSU/C/LIN/SANI). 2023-07-18 5.4 Media Vilnerability in the Oracle Agale Plus product of Oracle Supply Chain (component: Welchient). The supported version that is affected to 3.5 & 6.7918 vegolitotal vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agale Plus. Successful attacker require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agale Plus. Successful attacker require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agale Plus. Successful attack require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agale Plus Agazes was a supported additional power of Oracle Agale Plus Macassible datas a swell as unauthorised read access to a subset of Oracle Agale Plus Macassible datas as well as unauthorised read access to a subset of Oracle Agale Plus Macassible datas as well as unauthorised read access to a subset of Oracle Disease of Confedence o		oracle - multiple	·			
Vulnerability in the Oracle Agile PIM product of Oracle Supply Chain (component: Webfillent). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access shill PTID to compromise Oracle Agile PIM. Successful attacker of the univariability is in Oracle Agile PIM. Successful attacker of the univariability is in Oracle Agile PIM. Successful attacker of which we univariability is in Oracle Agile PIM. Successful attacker of the univariability is in Oracle Agile PIM. Successful attacker of the univariability can result in unauthorated update, insert or delete access to some of Oracle Agile PIM accessful the as sevel as unauthorized read of Oracle Agile PIM accessful the ass well as unauthorized read of Oracle Agile PIM accessful the ass well as unauthorized read oracle oracle agile plim oracle of Oracle Deletwins (Component: ELI O'Orbetrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability in the LD Edwards EnterpriseDen Orchestrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise ID Edwards EnterpriseDen Orchestrator accession of the universability and result in unauthorized update, insert or delete access to some of ID Edwards ExterpriseDen Orchestrator accession of this work or accessible data as well as unauthorized access to a subset of ID redwards ExterpriseDen Orchestrator accession access via the ID redwards ExterpriseDen Oracles ExterpriseDen Oracles ExterpriseDen Oracles ExterpriseDen Oracles ExterpriseDen Oracles ExterpriseDen Oracles Exte	CVE-2023-22020	· ·		2023-07-18	5.4	Medium
affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access a laTTIP to compromise Oracle Agile PLM. Successful attacks or fluid wulnerability is in Oracle Agile PLM. Successful attacks or fluid wulnerability is in Oracle Agile PLM. Attacks may significantly impact additional products (society attacks of this wulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.1 Base Society S. (Confloitentiality and Integrity impacts). CVSS Vulnerability in the 10 Edwards Enterprised Plant and State and Prior to 9.2.74. Easily exploitable vulnerability allows low privileged attacker with metwors access via HTTP to compromise Defarration. Successful attacks of this vulnerability and result in unauthorized update, paster or delete access to oracle of 10 Edwards Enterprised Plant Control and State and Sta		,				
privileged attacker with network access via HTTP to compromise Oracle Agale PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agale PLM, accessful attacks of this vulnerability can result in unauthorized update, insert of delete access to some of Grade Agale PLM accessible GHA access to south and access to assist of Oracle Agale PLM accessible GHA access to assist of Oracle Agale PLM accessible GHA access to some of Grade Agale PLM accessible GHA access to some of Grade Agale PLM accessible GHA accessible G			Chain (component: WebClient). The supported version that is			
Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM. Attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. Scv 53: 1 838 Score 5.4 (Confidentiality and integrity impacts). CVS VLC VCVS-3.21AVM/ACL/PRIL/UIR/SC/CL/I-I/L/AN). 2023-07-18 5.4 Medit Vulnerability is the DI Edwards (temporent: EL IOT Orchestrator Security). Supported version that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows for privated art tacher with network access with HTT to compromise DI Edwards EnterpriseOne Orchestrator Security. Supported version that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows for privated attacker with network access with HTT to compromise DI Edwards EnterpriseOne Orchestrator vulnerability can result in unauthorized quadact, insert or delete access to some of ID Edwards EnterpriseOne Orchestrator vulnerability and integrity impacts). CVS Vector (CVS-3.3.1AVMACL/PRIL/UIR/SVS/CLVI/LA/N). 2023-07-18 5.4 Medit Vector (CVS-3.3.1AVMACL/PRIL/UIR/SVS/CLVI/LA/N). 2023-07-19 5.4 Medit Vector (CVS-3.3.1AVMACL/PRIL/UIR/SVS/CLVI/LA/N). 2023-07-19 5.4 Medit Vector (CVS-3.3.1AVMACL/PRIL/UIR/SVS/CLVII/LA/N). 2023-07-19 5.4 Medit Vector (CVS-3.3.1AVMACL/PRIL/UIR/			affected is 9.3.6. Easily exploitable vulnerability allows low			
from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVS 3.1 Sass Soore 5.4 (Confidentiality and Integrity impacts). CVS Vector: (CVSS3.1)AVM/ACCIPATI. UNIFS/CCI./LI/LA/NN). Vulnerability in the ID Edwards Enterprise One Orchestrator product of Oracle De Edwards Component: E11 OT Orchestrator Security. Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows buy privileged attacker with network access via HTTP to compromise ID Edwards Enterprise One Orchestrator accessible data as well as unauthorized update; insert or delete access to some of ID Edwards Enterprise One Orchestrator Accessible data as well as unauthorized update; insert or delete accessible data as well as unauthorized read access to a subset of ID Edwards Enterprise One Orchestrator Accessible data as well as unauthorized read access to a subset of ID Edwards Enterprise One Orchestrator Accessible data as well as unauthorized read access to a subset of ID Edwards Enterprise One Orchestrator Accessible data as well as unauthorized read access to a subset of ID Edwards Enterprise Decorption (VSS 3.1) AVM/ACCIPATI. UNIV. SUZIVE/IJI./LIV. SUZIVE/IJI./LIV. SUZIVE/IJI./LIV. SUZIVE/IJI./LIV. NO. VOSS 3.1 AVM/ACCIPATI. UNIV. SUZIVE/IJI./LIV. NO. VOSS 3.1 AVM/ACCIPATI. UNIV. SUZIVE/IJI./LIV. NO. VOSS 3.1 AVM/ACCIPATI. UNIV. SUZIVE/IJI./LIV. NO. VOSS 3.1 AVM/ACCIPATI. VOSS 3.1 AVM/A			'			
is in Oracle Agile PLM, attacks may significantly impact additional products (sospe change). Successful attacks or this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data (SVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially in the ID integrity of the PLM Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially can result in unauthorized update, insert or delete access to some of JD Edwards (component: E1 to To Crichestrator Soze 1.4 (Confidentially can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseCone Orchestrator accessible data. CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially and Integrity impacts). CVS 3.1 Base Soze 5.4 (Confidentially allows tow privileged attacker with network access to a subset of JD Confidentially allows tow privileged attacker with network access to a subset of Oracle Analytics (component: Visual Analyze). The supported version that is affected is 6.4.0.0.0 Exist year) by the CVE 2023-2026 (CVE 2023-2026). CVE			,			
products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVS 3.1 See Score 5. 4 (Confidentiality and integrity impacts). CVS Vector; (CVSS.3.1/A.V.MA.CL.PHZ.IULINS.SC.CL.PLIA.V.M.). Vulnerability in the Di Edwards Enterprise One Oracle Detwards Component: Et IC TO Orachestator product of Oracle Di Edwards (component: Et IC TO Orachestator Security). Supported versions that are affected are Prior to 9. 9.7.7.4. Easily exploitable vulnerability alions boy privileged attacker with network access via HTTP to compromise ID Edwards Enterprise Oraches Detwards access to some of ID Edwards Enterprise Orachestator accessible data as well as unauthorized update, insert or delete access to some of ID Edwards Enterprise Orachestator accessible data. CVSS 3.1 See Score 5. 4 (Confidentiality and integrity impacts). CVSS Vectors (CVSS.3.1/A.V.MA.CL.PHZ.IULINS.VIJC.LYII.A.V.M.). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Authoritics (Component: Visual Analyze). The supported version that is affected is 6.40.0.0. Easily exploitable vulnerability allows low privileged attacker with hetwork access via HTTP to compromise Oracle Business Intelligence Enterprise Edition, accessed and access to a subset of Oracle Authoritics (Component: Visual Analyze). The supported version that is affected is 6.40.0.0. Easily exploitable vulnerability allows low privileged attacker with hetwork access via HTTP to compromise Oracle Business Intelligence Enterprise Edition, accessed and as well as unauthorized update, insert or delete access to one of Oracle Business Intelligence Enterprise Edition accessed and as well as unauthorized update, insert or delete access to one of Oracle Business Intelligence Enterprise Edition accessed and as well as unauthorized update, insert or delete access to one of Oracle						
can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data or Not St. 3.1 Base Score 5.4 (Confidentially and Integrity impacts). CVS. Vivierability in the DI Cetwork St. Affording PLM Accessible data. CVSS.3.1 Base Score 5.4 (Confidentially in the DI Cetwork St. PLM						
Of Grade Agile PLM accessible data as well as unauthorized read access to a subset of 70 accel. Pagile PLM accessible data. CVSS 3.1 Bases Score S.4 (Confidentiality and Integrity impacts). CVSS 3.1 Bases Score S.4 (Confidentiality and Integrity impacts). CVSS 3.1 When the DE dwards EnterpriseDen Orchestrator product of Oracle ID Edwards (component: ELI DIOT Orchestrator Security). Supported versions that are affected are Prior to 3.2.7.4 Easily exploitable whereability allows low privileged attacker with network access via HTTP to compromise ID Edwards. EnterpriseDen Orchestrator Security). Supported versions that are affected are Prior to 3.2.7.4 Easily exploitable whereability allows low privileged attacker with network access via HTTP to compromise ID Edwards. Enterprise Den Orchestrator Some of ID Edwards. Enterprise Den Orchestrator Some of ID Edwards EnterpriseDen Orchestrator Accessible data. Oxide Some of ID Edwards EnterpriseDen Orchestrator Accessible data as well as unauthorized update, insert or delete access to some of ID Edwards EnterpriseDen Orchestrator Accessible data. Oxide Some of ID Edwards EnterpriseDen Orchestrator Accessible data as well as unauthorized read access to a subset of Oxide Accessible data. Oxide Some of ID Edwards Enterprise Delibor or Accessible data accessible data. Oxide Some of ID Edwards Enterprise Delibor or Oxide Accessible data accessible						
access to a subset of Oracle Agile PLM accessible data CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS-3.1/AVN)ACL/PRI-L/URI/S/SC/CL/In1A/N). Voluneability in the De Edwards EnterpriseScore Orchestrator product of Oracle ID Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network accessive in HTD to compromise ID Edwards EnterpriseCone Orchestrator. Successful attacks of this: vulnerability can result in unauthorized updates, insert or delete access to some of JD Edwards EnterpriseCone Orchestrator. Successful attacks of this: vulnerability can result in unauthorized updates, insert or delete accessible data as well as unauthorized read access to a subset of jd_edwards_enterp insecone, orchestrator. Successful attacks of this: vulnerability can result in unauthorized read access to a subset of jd_edwards_enterp insecone, orchestrator. Successful attacks of this: vulnerability can result in unauthorized accessible data. CVSS 3.1 Vector: (CVSS-3.1/AVN)ACL/PRI-L/UNSV)CL/TL/IA/N.). Vector: (CVS-3.1/AVN)ACL/PRI-L/UNSV)CL/TL/IA/N.). Vector: (· · ·			
Saes Soore S. 4 (Confidentiality and Integrity impacts). CVS Vector: (CVSS-31/ANN/ACL/PRI-L/USI-S/CC/L/USI-AN). Vulnerability in the D Edwards EnterpriseOne Orchestrator product of Oracle ID Edwards (component: 16 107 Orchestrator Security). Supported versions that are affected are Prior to 3.2.7.4 Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise ID Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized access to subset of Id edwards_enterp in JC Edwards. EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of Id edwards_enterp in JC Edwards EnterpriseOne Orchestrator accessible data as vell as unauthorized read access to a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as unauthorized read access to a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as unauthorized read access to a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as a subset of ID Edwards EnterpriseOne Orchestrator accessible data as vell as unauthorized read access to a subset of ID Edwards Enterprise Edition product Score Compromise Oracle Business Intelligence Enterprise Edition accessible data as excess to a subset of ID Edwards Enterprise Edition, attacks may significantly impact additional products Score change, Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to a subset of Oracle Business Intelligence Enterprise Edition, attacks and while the vulnerability in Coracle Edwards Enterprise Edition, attacks may significantly impact additional products Score change in Edwards Enterprise Edition, attacks may significantly impact additional products Sco						
Vectors (CVS-3-12/AVN)ACL/REA/L/URIS/SC/CL/In1/AN). 2023-07-18 5.4 Media Vulnerability in the DE dwards Enterprise Color Orchestrator product of Oracle JD Edwards (component: El JOT Orchestrator Security.) Supported versions that are affected are Prior to 3.2.7.4 Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator Security. Security Component: El JOT Oracles attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator Security. Security Securi						
Vulnerability in the JD Edwards EnterpriseOne Orchestrator Security . Supported versions that are affected are Prior to 9.27.A. Easily exploitable unlareability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1	C//F_2022 22020	oracle agile alm		2022 07 10	E 1	Modium
product of Oracle JD Edwards (component: ELIOT Orchestrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise ID Edwards. Enterprise-One Orchestrator. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of ID Edwards Enterprise-One Orchestrator accessible data as well as unauthorized update, insert or delete access to so some of ID Edwards Enterprise-One Orchestrator accessible data as well as unauthorized read access to a subset of jd_edwards_enterprise-One Orchestrator accessible data composition or orchestrator or Vector. (CVS-33.1/ANN/ACL/PRE/ULINE/SU/CL/IA/AN). 2023-07-18 5.4 Media Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analysics (component: Visual Analysey). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition accessible data service in the Visual Analysey. The supported version that is affected as Edwards with responsibility and interprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as well as unauthorized read access to a subset of Oracle Busin	CVL-2025-22039	oracie - agile_pim		ZUZ3-U/-18	3.4	ivieuluffi
Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable ulumerability allows low privileged attacker with network access via HTTP to compromise ID Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized update, insert or delete access to accessible data as well as unauthorized read access to a subset of jd_edwards_enterpriseOne Orchestrator accessible data. CVSS 3.1 accessible data as well as unauthorized read access to a subset of jd_edwards_enterpriseOne Orchestrator accessible data. CVSS 3.1 accessible data as well as unauthorized read access to a subset of jd_edwards_enterpriseOne Orchestrator accessible data. CVSS 3.1 accessible data as well as unauthorized predate, insert or delete access to a subset of jd_edwards_enterpriseOne Orchestrator accessible data. CVSS 3.1 accessible data as well as a fetched is 6.4 0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data acc			· · · · · · · · · · · · · · · · · · ·			
9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise DF Bdwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized quadate, insert or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of jd_edwards_enterp. JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of jd_edwards_enterp. JD Edwards EnterpriseOne Orchestrator accessible data. CVSS-3.1/ANNACL/PRE/LUNINS/UCL/LI/LAN). 2023-07-18 5.4 Medit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition product of Oracle Analysics (component: Visual Analyse). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition Oracle Business Intelligence Enterprise Edition accessible data. See the province of t						
attacker with network access via HTTP to compromise ID Edwards EnterpriseOne Orchestrator . Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of ID Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of ID Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Bases Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS.3.1/AV:N/ACL/PR:L/ULN/S:J/CL/It-L/AN). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4 0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as vell as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as explained accessible data as vell as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as explained accessible data as vell as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as Explained Enterprise Edition accessible data as Explained Enterprise Edition accessible data as Explained Enterprise Edition accessible data accessible at Explained Enterprise Edition accessible data accessible at Explained Enterprise Edition accessible data accessible at Explained Enterp						
EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS.31.4/AVN/ACL/PRI.U/NS.VIJC.LIV.LAN). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to so moe of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and integrity impacts). CVSS Vector: (VE-2023-22061 cell business intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and integrity impacts). CVSS Vector: (VE-2023-23043 escore 5.4 (Confidentiality and integrity impacts). CVSS Vector: (VE-2023-23040 stell) in the oracle Business intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and integrity impacts). CVSS Vector: (VE-2023-23040 stell) in the delete of the CVE-2023-23040 stell in the CVE-2023-23040 stell) in the CVE-2023-23040 stell in t						
vulnerability can result in unauthorized update, insern or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and integrity impacts). CVSS Vector: (CVSS.3.1/AV.N/ACI./PRI./UN.N/S.U/C.I/I:L/A.N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful Lattacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business intelligence Enterprise Edition accessible data access to a subset of Oracle Business			· ·			
access to some of JD Edwards EnterpriseOne Orchestrator oracle jd_edwards_entery riseone_orchestrato or			·			
oracle - id_edwards_enterp						
riseone_orchestrat Vector: (CVSS.3.1/AV:N/ACI./PR:L/ULN/S:U/CL1/:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to osome of Oracle Business Intelligence Enterprise Edition accessible data cvSS 3.1 Base Score 5.4 (Confidentiality and integrity impacts). CvSS Vector. (VE-2023-22061 ce VE-2023-22061 ce IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be rusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X- Fore ID: 252186. UKE-2023-29260 IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server- side request forger (SSR). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker to send unauthorized request strom the system, potentially leading to network enumeration or facilitating other attacker to send unauthorized request strom the system, potentially leading to network enumeration or facilitating othe		oracle -	·			
vettor: (CVS-3.3_IAV-N)AC-I_VPR.I_VII.N_S-I_VC-I_I-I_I_AN). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business intelligence Enterprise Edition accessible products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a Base Secretor Secretion to visit a specially oracle data access to a subset of Oracle Business Intelligence Enterprise Edition accessible data access to a Bas			·			
Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.1 Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, Attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: CVE-2023-22061 ce (CVSS.3.1/AN:A/AC.I./PR.I./UIR/Sr.C/C.I./I.I./A.N). 2023-07-18 5.4 Media (CVE-2023-22061 ce (CVSS.3.1/AN:A/AC.I./PR.I./UIR/Sr.C/C.I./I.A.N). 2023-07-18 5.4 Media (CVE-2023-22061 ce (CVSS.3.1/AN:A/AC.I./PR.I./UIR/Sr.C/C.I./I.I./A.N). 2023-07-18 5.4 Media (CVE-2023-22061 ce (CVSS.3.1/AN:A/AC.I./PR.I./UIR/Sr.C/C.I./I.I./A.N). 2023-07-19 5.4 Media (CVE-2023-22061 ce (CVS.3.1/AN:A/AC.I./PR.I./UIR/Sr.C/C.I./I.I./A.N). 2023-07-19 5.4 Media (CVE-2023-22060 ce (CVE-2023-22060 c		riseone_orchestrat	, , , ,			
product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition accession attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: CVE-2023-22061 ce (CVSS.3.1/AN/ACL/PR.L/UR.KS/C.C/LI/LA/N). 2023-07-18 5.4 Medit or redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-force ID: 252136. Security_verify_acc ess IBM Stering Connect: Express for UNIX 1.5 is vulnerable to servers side request foregry (SSRP). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to retwork enumeration or facilitating other attacks. IBM X-force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability vulnerability to execute scripts	CVE-2023-22050	or		2023-07-18	5.4	Medium
supported version that is affected is 6.4.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS 2.1/AV:NA/AC:L/PR:L/ULR;RS:C/CLI/It./A:N). CVE-2023-22061 CVE-2023-22061 CVE-2023-230433 EDITION OR COMPARIANCE COMPAIL OR						
vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 33.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVE-2023-22061 ce (CVSS:3.1/AV:N/Acc.I/PR:/UI:R/S:C/CL!/LI:L/A:N). IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker coolatin highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. CVE-2023-30433 ess Force ID: 252186. IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker in the system of th			, , , , , , , , , , , , , , , , , , , ,			
HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: CVE-2023-22061 Ce (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-security. Verify_acc ess CVE-2023-30433 ess Force ID: 252186. IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSR). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. CVE-2023-29260 sterling_connect! BIM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. BIM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker c						
Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVE-2023-22061 ce (CVSS:3.1AVA/NaCL/PRL/INF/SC/CL/IL/LA/N). 2023-07-18 5.4 Medit and integrity impacts). CVSS Vector: (CVE-2023-22061 ce (CVSS:3.1AVA/NaCL/PRL/INF/SC/CL/IL/LA/N). 2023-07-18 5.4 Medit ibm - scurity_verify_acc attack as personal or a victim to visit as specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-force ID: 252186. [BM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker. IBM X-force ID: 252135. [BM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-force ID: 247861. [BM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations						
person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVS:3.1/AV:N/Act./PR:L/UI:R/S:C/C:L/I:L/A:N). 2023-07-18 5.4 Medit IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL diplayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-force ID: 252186. 2023-07-19 5.4 Medit Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker to send unauthorized requests from the system, potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerablity leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a vic						
Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVE-2023-22061 ce (CVSS:3.1/AV:N/AC:L/PRI-L/U:R/S:C/C:L/I-L/A:N). 2023-07-18 5.4 Medic Medical Med						
significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVE-2023-22061 ce (CVSS.3.1/AV:N/AC:L/PR:L/U:R/S:C/C:L/I:L/A:N). 2023-07-18 5.4 Medic IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-proce ID: 252186. 2023-07-19 5.4 Medic IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. BIBM X-proce ID: 252135. 2023-07-19 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-proce ID: 247861. 2023-07-22 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to excute scripts in a victim's Web browser within the security context of the hosting Web site. An a						
attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVS-2023-22061 ce (CVSS:3.1/AV:N/AC:I./PR:I./UI:R/S:C/C:I./I:I./A:N). 2023-07-18 5.4 Medic CVSS 3.1/AV:N/AC:I./PR:I./UI:R/S:C/C:I./I:I./A:N). IBM Security Verify Access 1.0. could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. CVE-2023-30433 ess IBM Selection Conduct Further attacks against the victim. IBM X-Force ID: 252186. DIBM Selection Conduct further attacks against the victim. IBM X-Force ID: 252185. DIBM Selection Conduct further attacks against the victim. IBM X-Force ID: 252135. DIBM Selection Conduct further attacks against the victim. IBM X-Force ID: 252135. DIBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerablity 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: 247861. DIBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to excute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			· · · · · · · · · · · · · · · · · · ·			
insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVF-2023-22061 ce (CVS:3.1/AV:N/AC:L/PR:L/U:R/S:C/C:L/I:L/A:N)). 2023-07-18 5.4 Medic IBM Security Verify Access 1.0. could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-force ID: 252186. 2023-07-19 5.4 Medic IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-force ID: 252135. 2023-07-19 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this						
Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. CVE-2023-30433 ess IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252185. LBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. CVE-2023-25929 products IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this						
access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVS:3.1/AV:N/AC:L/PR:L/U:R/S:C/C:L/I:L/A:N). IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X- Force ID: 252186. VE-2023-30433 BIM Sterling Connect:Express for UNIX 1.5 is vulnerable to server- side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacker. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross- site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			_			
oracle - business_intelligen Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVE-2023-22061 Ce						
business_intelligen ce (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). BM Security Verify Access 1.0.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. BM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. BM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. BM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this		oracle -	,			
CVE-2023-22061 ce (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). 2023-07-18 5.4 Medic IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-force ID: 252186. 2023-07-19 5.4 Medic attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-force ID: 252135. 2023-07-19 5.4 Medic attacks. IBM X-force ID: 252135. 2023-07-19 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-force ID: 247861. 2023-07-22 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit us this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			· · · · · · · · · · · · · · · · · · ·			
IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this	CVE-2023-22061			2023-07-18	5.4	Medium
conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. CVE-2023-30433 ess IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. BM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this						1
persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. CVE-2023-30433 ess IBM Sterling Connect: Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			· · ·			
attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. 2023-07-19 5.4 Medit IBM Sterling Connect: Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. 2023-07-19 5.4 Medit IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Medit IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this						
ibm - security_verify_acc ess						
security_verify_acc ess information or conduct further attacks against the victim. IBM X- Force ID: 252186. 2023-07-19 5.4 Medic IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server- side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. 2023-07-19 5.4 Medic IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Medic CVE-2023-25929 IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross- site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			• •			
CVE-2023-30433 ess Force ID: 252186. 2023-07-19 5.4 Media IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server- side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. 2023-07-19 5.4 Media IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Media CVE-2023-25929 products IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			_ ·			
IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server- side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross- site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this		security_verify_acc				
side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this	CVE-2023-30433	ess		2023-07-19	5.4	Medium
attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. CVE-2023-25929 Products IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			· ·			
ibm - sterling_connect\ attacks. IBM X-Force ID: 252135. 2023-07-19 5.4 Media attacks. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Media IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			, , , , ,			
CVE-2023-29260 sterling_connect\ attacks. IBM X-Force ID: 252135. 2023-07-19 5.4 Media IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Media IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this		.,				
IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Mediu IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this	CVE 2022 2022		1	2022 07 42	F 4	p.a1*
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: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross- site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this	CVE-2023-29260	steriing_connect\		2023-07-19	5.4	Medium
JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored crosssite scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			,			
ibm - multiple products functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Media IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this						
CVE-2023-25929 products trusted session. IBM X-Force ID: 247861. 2023-07-22 5.4 Media IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross- site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this		ihm - multiple	, · · · · · · · · · · · · · · · · · · ·			
IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross- site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this	CVF-2023-25020	•		2023-07-22	5 /	Medium
site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this	CVL-2023-23929	products		2023-07-22	3.4	ivieululli
Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			,			
execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this			, , , ,			
context of the hosting Web site. An attacker could use this			·			
		ibm - multiple	vulnerability to steal the victim's cookie-based authentication			
	CVE-2023-28530	•	· ·	2023-07-22	5.4	Medium

	I				T
0.42	ibm - infosphere_informa	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-	2222 27 47		
CVE-2023-33857	tion_server	Force ID: 257695. IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass	2023-07-17	5.3	Medium
CVE-2023-35901	ibm - multiple products	which could allow invalid changes or values in some fields. IBM X-Force ID: 259380.	2023-07-17	5.3	Medium
		Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server.			
		For the application to be affected, it needs to satisfy the following requirements:			
		* It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses. * The application infrastructure does not guard against clients submitting (X-)Forwarded headers.			
CVE-2023-34036	vmware - multiple products		2023-07-17	5.3	Medium
CVL 2023 34030	products	Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to methods on @Controller-annotated classes.)	2023 07 17	3.3	Wicdiani
		Specifically, an application is vulnerable when all of the following are true:			
		* Spring MVC is on the classpath * Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet) * The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints			
		An application is not vulnerable if any of the following is true:			
		* The application does not have Spring MVC on the classpath * The application secures no servlets other than Spring MVC's DispatcherServlet * The application uses requestMatchers(String) only for Spring MVC endpoints			
CVE-2023-34035	vmware - multiple products		2023-07-18	5.3	Medium
	ibm - multiple	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force			
CVE-2023-35900	products	ID: 259368.	2023-07-19	5.3	Medium
CVE-2023-29259	ibm - sterling_connect\	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055. Issue summary: Checking excessively long DH keys or parameters may be very slow.	2023-07-19	5.3	Medium
		Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.			
		The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a			
CVE-2023-3446	openssl - multiple products	modulus which is over 10,000 bits in length.	2023-07-19	5.3	Medium

However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or	
key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or	
modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or	
even if it has already been found to be too large. An application that calls DH_check() and supplies a key or	
An application that calls DH_check() and supplies a key or	
parameters obtained from an untrusted source could be vulernable to a Denial of	
Service attack.	
The function DH sheek() is itself called by a number of other	
The function DH_check() is itself called by a number of other OpenSSL functions.	
An application calling any of those other functions may similarly be	
affected. The other functions affected by this are DH_check_ex() and	
EVP_PKEY_param_check().	
Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications	
when using the '-check' option.	
The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this	
issue.	
Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	
Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are	
Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle	
GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle	
GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the	
infrastructure where Oracle Java SE, Oracle GraalVM Enterprise	
Edition, Oracle GraalVM for JDK executes to compromise Oracle	
Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in	
unauthorized access to critical data or complete access to all	
Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java	
deployments, typically in clients running sandboxed Java Web	
Start applications or sandboxed Java applets, that load and run	
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply	
to Java deployments, typically in servers, that load and run only	
trusted code (e.g., code installed by an administrator). CVSS 3.1	
oracle - multiple Base Score 5.1 (Confidentiality impacts). CVSS Vector: CVE-2023-22041 products (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). 2023-07-18 5.1	Medium
Vulnerability in the MySQL Server product of Oracle MySQL	Wiedidiii
(component: Server: Replication). Supported versions that are	
affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols	
to compromise MySQL Server. Successful attacks of this	
vulnerability can result in unauthorized ability to cause a hang or	
frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	
CVE-2023-21950 oracle - mysql (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). 2023-07-18 4.9	Medium
Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are	
affected are 5.7.41 and prior and 8.0.32 and prior. Easily	
exploitable vulnerability allows high privileged attacker with	
network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	
unauthorized ability to cause a hang or frequently repeatable	
crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	
oracle - multiple (Availability impacts). CVSS Vector: CVE-2023-22007 products (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). 2023-07-18 4.9	Medium
Vulnerability in the MySQL Server product of Oracle MySQL	
(component: InnoDB). Supported versions that are affected are	
8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	
compromise MySQL Server. Successful attacks of this vulnerability	
can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base	
Score 4.9 (Availability impacts). CVSS Vector:	
CVE-2023-22008 oracle - mysql (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). 2023-07-18 4.9	Medium
Vulnerability in the Unified Audit component of Oracle Database	

		T	T		1
		Net to compromise Unified Audit. Successful attacks of this			
		vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Unified Audit accessible			
		data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector:			
		(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).			
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows			
		high privileged attacker with network access via multiple protocols			
		to compromise MySQL Server. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or			
		frequently repeatable crash (complete DOS) of MySQL Server.			
CVE 2022 22046		CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	2022 07 40	4.0	Madium
CVE-2023-22046	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the MySQL Server product of Oracle MySQL	2023-07-18	4.9	Medium
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.33 and prior. Easily exploitable vulnerability allows			
		high privileged attacker with network access via multiple protocols			
		to compromise MySQL Server. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.			
		CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:			
CVE-2023-22054	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.9	Medium
	, ,	Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.33 and prior. Easily exploitable vulnerability allows			
		high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or			
		frequently repeatable crash (complete DOS) of MySQL Server.			
0.45.0000.55		CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	2225		
CVE-2023-22056	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are			
		affected are 8.0.33 and prior. Easily exploitable vulnerability allows			
		high privileged attacker with network access via multiple protocols			
		to compromise MySQL Server. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or			
		frequently repeatable crash (complete DOS) of MySQL Server.			
CVE-2023-22057	oracle - mysql	CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.9	Medium
<u> </u>					
	dell -	Wyse Management Suite versions prior to 4.0 contain an improper			
0.45 0000 00400	wyse_management	authorization vulnerability. An authenticated malicious user with			
CVE-2023-32482	_suite	privileged access can push policies to unauthorized tenant group. IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local	2023-07-20	4.9	Medium
	ibm - multiple	user to cause a denial of service due to due to improper time-of-			
CVE-2023-33832	products	check to time-of-use functionality. IBM X-Force ID: 256012.	2023-07-19	4.7	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Replication). Supported versions that are			
		affected are 8.0.33 and prior. Difficult to exploit vulnerability			
		allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or			
		frequently repeatable crash (complete DOS) of MySQL Server.			
0.45.0000.55		CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector:	2225		
CVE-2023-22005	oracle - mysql	(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.4	Medium
		Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that			
		are affected are 14.1.1.0.0 and 12.2.1.4.0. Difficult to exploit			
		vulnerability allows high privileged attacker with network access			
		via T3, IIOP to compromise Oracle WebLogic Server. Successful			
		attacks of this vulnerability can result in unauthorized ability to			
		cause a hang or frequently repeatable crash (complete DOS) of			
	oracle - multiple	Oracle WebLogic Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector:			
CVE-2023-22031	products	(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.4	Medium
	,	Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: InnoDB). Supported versions that are affected are			
		8.0.33 and prior. Difficult to exploit vulnerability allows high			
		privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability			
		can result in unauthorized ability to cause a hang or frequently			
		repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base			
	İ	Score 4.4 (Availability impacts). CVSS Vector:			
		, , , , ,			
CVE-2023-22033	oracle - mysql	(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.4	Medium
CVE-2023-22033	oracle - mysql	(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the MySQL Server product of Oracle MySQL	2023-07-18	4.4	Medium
CVE-2023-22033 CVE-2023-22058	oracle - mysql oracle - mysql	(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	4.4	Medium Medium

	T				ı
		privileged attacker with network access via multiple protocols to			
		compromise MySQL Server. Successful attacks of this vulnerability			
		can result in unauthorized ability to cause a hang or frequently			
		repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base			
		Score 4.4 (Availability impacts). CVSS Vector:			
		(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).			
		NAVian Managamant Cuita vanciana muianta 4.0 aantain a aansitiva			
		Wyse Management Suite versions prior to 4.0 contain a sensitive			
	-1 - 11	information disclosure vulnerability. An authenticated malicious			
	dell -	user having local access to the system running the application			
CVE 2022 22492	wyse_management	could exploit this vulnerability to read sensitive information	2023-07-20	4.4	Modium
CVE-2023-32483	_suite	written to log files. Vulnerability in the Oracle Applications Technology product of	2023-07-20	4.4	Medium
		Oracle E-Business Suite (component: Reports Configuration).			
		Supported versions that are affected are 12.2.3-12.2.12. Easily			
		exploitable vulnerability allows unauthenticated attacker with			
		network access via HTTP to compromise Oracle Applications			
		Technology. Successful attacks require human interaction from a			
		person other than the attacker. Successful attacks of this			
		vulnerability can result in unauthorized update, insert or delete			
		access to some of Oracle Applications Technology accessible data.			
	oracle - e-	CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector:			
CVE-2023-22004	business suite	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2023-07-18	4.3	Medium
<u> </u>	Susiness_suite	Vulnerability in the Oracle Self-Service Human Resources product	2023 07-10	7.5	MICUIUIII
		of Oracle E-Business Suite (component: Workforce Management).			
		Supported versions that are affected are 12.2.3-12.2.12. Easily			
		exploitable vulnerability allows low privileged attacker with			
		network access via HTTP to compromise Oracle Self-Service			
		Human Resources. Successful attacks of this vulnerability can			
		result in unauthorized read access to a subset of Oracle Self-			
	oracle - self-	Service Human Resources accessible data. CVSS 3.1 Base Score 4.3			
	service_human_res	(Confidentiality impacts). CVSS Vector:			
CVE-2023-22009	ources	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	4.3	Medium
	33000	Vulnerability in the Oracle Business Intelligence Enterprise Edition			
		product of Oracle Analytics (component: Analytics Server). The			
		supported version that is affected is 7.0.0.0.0. Easily exploitable			
		vulnerability allows low privileged attacker with network access via			
		HTTP to compromise Oracle Business Intelligence Enterprise			
		Edition. Successful attacks of this vulnerability can result in			
		unauthorized update, insert or delete access to some of Oracle			
	oracle -	Business Intelligence Enterprise Edition accessible data. CVSS 3.1			
	business_intelligen	Base Score 4.3 (Integrity impacts). CVSS Vector:			
CVE-2023-22012	ce	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	4.3	Medium
		Vulnerability in the Oracle Business Intelligence Enterprise Edition			
		product of Oracle Analytics (component: Analytics Server).			
		Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0.			
		Easily exploitable vulnerability allows low privileged attacker with			
		network access via HTTP to compromise Oracle Business			
		Intelligence Enterprise Edition. Successful attacks of this			
		vulnerability can result in unauthorized update, insert or delete			
		access to some of Oracle Business Intelligence Enterprise Edition			
	oracle - multiple	accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS			
CVE-2023-22013	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	4.3	Medium
		Vulnerability in the Oracle Business Intelligence Enterprise Edition			
		product of Oracle Analytics (component: Analytics Server).			
		Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0.			
		Easily exploitable vulnerability allows low privileged attacker with			
		network access via HTTP to compromise Oracle Business			
		Intelligence Enterprise Edition. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a partial			
		denial of service (partial DOS) of Oracle Business Intelligence			
0) /5 0000 0000	oracle - multiple	Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts).	2022 2- :-		
CVE-2023-22021	products	CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2023-07-18	4.3	Medium
		Vulnerability in the Oracle Business Intelligence Enterprise Edition			
		product of Oracle Analytics (component: Analytics Server). The			
		supported version that is affected is 7.0.0.0.0. Easily exploitable			
		vulnerability allows low privileged attacker with network access via			
		HTTP to compromise Oracle Business Intelligence Enterprise			
		Edition. Successful attacks of this vulnerability can result in			
	oracle	unauthorized ability to cause a partial denial of service (partial			
	oracle -	DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1			
CVE_2022 22027	business_intelligen	Base Score 4.3 (Availability impacts). CVSS Vector:	2022 07 10	ΛЭ	Madium
CVE-2023-22027	ce	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). Vulnerability in the Oracle VM VirtualBox product of Oracle	2023-07-18	4.3	Medium
		Virtualization (component: Core). Supported versions that are			
		affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable			
		vulnerability allows high privileged attacker with logon to the			
		infrastructure where Oracle VM VirtualBox executes to			
	oracle - multiple	compromise Oracle VM VirtualBox. Successful attacks require			
İ		human interaction from a person other than the attacker.	2023-07-18	4.2	Medium
CVE-2023-22016	products	I HUHIAH IIHETACHON MONI A DERSON OMER MAN ME AMARKET		4,	MEULLIN

		6 61 11 1 611 1 1 1 1 1 1 1 1 1 1 1 1 1		- 1	
		Successful attacks of this vulnerability can result in unauthorized			
		ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.2 (Availability			
		impacts). CVSS Vector:			
		(CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).			
		Vulnerability in the Advanced Networking Option component of			
		Oracle Database Server. Supported versions that are affected are			
		19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows			
		unauthenticated attacker with network access via Oracle Net to			
		compromise Advanced Networking Option. Successful attacks of			
		this vulnerability can result in unauthorized update, insert or			
	oracle - multiple	delete access to some of Advanced Networking Option accessible data. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector:			
CVE-2023-21949	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	3.7	Low
012 2023 213 13	products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	2020 07 10	3.7	2011
		Edition, Oracle GraalVM for JDK product of Oracle Java SE			
		(component: Utility). Supported versions that are affected are			
		Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise			
		Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and			
		20.0.1. Difficult to exploit vulnerability allows unauthenticated			
		attacker with network access via multiple protocols to			
		compromise Oracle Java SE, Oracle GraalVM Enterprise Edition,			
		Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service			
		(partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition,			
		Oracle GraalVM for JDK. Note: This vulnerability can be exploited			
		by using APIs in the specified Component, e.g., through a web			
		service which supplies data to the APIs. This vulnerability also			
		applies to Java deployments, typically in clients running sandboxed			
		Java Web Start applications or sandboxed Java applets, that load			
		and run untrusted code (e.g., code that comes from the internet)			
	arada multinla	and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7			
CVE-2023-22036	oracle - multiple products	(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	2023-07-18	3.7	Low
CAT 5052,5500	products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	202J-07-10	٥./	LUVV
		Edition, Oracle GraalVM for JDK product of Oracle Java SE			
		(component: Hotspot). Supported versions that are affected are			
		Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM			
		Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7			
		and 20.0.1. Difficult to exploit vulnerability allows			
		unauthenticated attacker with network access via multiple			
		protocols to compromise Oracle Java SE, Oracle GraalVM			
		Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a			
		subset of Oracle Java SE, Oracle GraalVM Enterprise Edition,			
		Oracle GraalVM for JDK accessible data. Note: This vulnerability			
		can be exploited by using APIs in the specified Component, e.g.,			
		through a web service which supplies data to the APIs. This			
		vulnerability also applies to Java deployments, typically in clients			
		running sandboxed Java Web Start applications or sandboxed Java			
		applets, that load and run untrusted code (e.g., code that comes			
	oracla multiple	from the internet) and rely on the Java sandbox for security. CVSS			
CVE-2023-22044	oracle - multiple products	3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.7	Low
CVL-2023-22044	products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	2023-U/-10	٥./	LUW
		Edition, Oracle GraalVM for JDK product of Oracle Java SE			
		(component: Hotspot). Supported versions that are affected are			
		Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle			
		GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle			
		GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit			
		vulnerability allows unauthenticated attacker with network access			
		via multiple protocols to compromise Oracle Java SE, Oracle			
		GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful			
		attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition,			
		Oracle GraalVM for JDK accessible data. Note: This vulnerability			
		can be exploited by using APIs in the specified Component, e.g.,			
		through a web service which supplies data to the APIs. This			
		vulnerability also applies to Java deployments, typically in clients			
		running sandboxed Java Web Start applications or sandboxed Java			
		applets, that load and run untrusted code (e.g., code that comes			
	amesta o to t	from the internet) and rely on the Java sandbox for security. CVSS			
CVE 2022 22045	oracle - multiple	3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector:	2022 07 40	י כ	Lave
CVE-2023-22045	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.7	Low
		Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE			
		(component: Libraries). Supported versions that are affected are			
		Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle			
	debian - multiple	GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle			
CVE-2023-22049	products	GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit	2023-07-18	3.7	Low

	Г				
		vulnerability allows unauthenticated attacker with network access			
		via multiple protocols to compromise Oracle Java SE, Oracle			
		GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful			
		attacks of this vulnerability can result in unauthorized update,			
		insert or delete access to some of Oracle Java SE, Oracle GraalVM			
		Enterprise Edition, Oracle GraalVM for JDK accessible data. Note:			
		This vulnerability can be exploited by using APIs in the specified			
		Component, e.g., through a web service which supplies data to the			
		APIs. This vulnerability also applies to Java deployments, typically			
		in clients running sandboxed Java Web Start applications or			
		sandboxed Java applets, that load and run untrusted code (e.g.,			
		code that comes from the internet) and rely on the Java sandbox			
		for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS			
		Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).			
_		Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle			
		GraalVM for JDK product of Oracle Java SE (component: GraalVM			
		Compiler). Supported versions that are affected are Oracle			
		GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for			
		JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows			
		unauthenticated attacker with network access via multiple			
		protocols to compromise Oracle GraalVM Enterprise Edition,			
		Oracle GraalVM for JDK. Successful attacks of this vulnerability can			
		result in unauthorized read access to a subset of Oracle GraalVM			
		Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS			
	oracle - multiple	3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector:			
CVE-2023-22051	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.7	Low
CVE-2023-22031	products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	2023-07-16	3.7	LOW
		Edition, Oracle GraalVM for JDK product of Oracle Java SE			
		(component: Networking). Supported versions that are affected			
		are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM			
		Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK:			
		17.0.7 and 20.0.1. Difficult to exploit vulnerability allows			
		unauthenticated attacker with network access via multiple			
		•			
		protocols to compromise Oracle Java SE, Oracle GraalVM			
		Enterprise Edition, Oracle GraalVM for JDK. Successful attacks			
		require human interaction from a person other than the attacker.			
		Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle			
		GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible			
		data. Note: This vulnerability applies to Java deployments, typically			
		in clients running sandboxed Java Web Start applications or			
		sandboxed Java applets, that load and run untrusted code (e.g.,			
		code that comes from the internet) and rely on the Java sandbox			
		for security. This vulnerability does not apply to Java deployments,			
		typically in servers, that load and run only trusted code (e.g., code			
		installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity			
CVE 2022 2200C	oracle - multiple	impacts). CVSS Vector:	2022 07 40	2.4	1
CVE-2023-22006	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2023-07-18	3.1	Low
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Pluggable Auth). Supported versions that are			
		affected are 8.0.33 and prior. Difficult to exploit vulnerability			
		allows low privileged attacker with network access via multiple			
		protocols to compromise MySQL Server. Successful attacks of this			
		vulnerability can result in unauthorized read access to a subset of			
		MySQL Server accessible data. CVSS 3.1 Base Score 3.1			
CVE 2022 22049	oraclo musal	(Confidentiality impacts). CVSS Vector:	2022 07 10	2.1	Low
CVE-2023-22048	oracle - mysql	(CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.1	Low
		Vulnerability in the Java VM component of Oracle Database			
	oracle - multiple	Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. CVSS Vector:			
CVE_2022 22052	· '		ეტევ_ტუ 10	2 1	Low
CVE-2023-22052	products	(CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	3.1	Low
		Vulnerability in the MySQL Server product of Oracle MySQL			
CVE 2022 22020	oracla marral	(component: Server: Security: Privileges). CVSS Vector:	2022 07 40	2.7	1
CVE-2023-22038	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	2.7	Low
		Vulnerability in Oracle Essbase (component: Security and			
CVE-2023-22010	oracle - essbase	Provisioning). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	2.2	Low
CAT-5052-55010	UI acie - ESSDASE	(CV33.3.1/AV.N/AC.H/FN.H/ULN/3.U/C.L/1.N/A.N).	2023-07-10	۷.۷	Low

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's دواذ تبقى NIST's المناسبة. NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.