

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 السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة national interests, NCA provides the weekly summary of published 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 15th المربوع من 10 اكتوبر إلى National Vulnerability Database (NVD) of October to 21st of October. Vulnerabilities are scored using the Common اكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) standard as per the حيث يتم تصنيف الثغرات بناء على Vulnerability Scoring System (CVSS) following severity:

Critical: CVSS base score of 9.0-10.0 High: CVSS base score of 7.0-8.9 Medium: CVSS base score 4.0-6.9 Low: CVSS base score 0.0-3.9

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
		Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system.			
		For steps to close the attack vector for this vulnerability, see the Recommendations section of this advisory			
CVE-2023-20198	cisco - ios_xe	Cisco will provide updates on the status of this investigation and when a software patch is available.	2023-10-16	10	Critical
372 2020 20200	5.555 103_XC	An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for	2020 10 10		Citical
CVE-2023-45871	linux - linux_kernel	frames larger than the MTU.	2023-10-15	9.8	Critical
CVE-2023-33836	ibm - security_verify_gov ernance	IBM Security Verify Governance 10.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 256016.	2023-10-16	9.8	Critical
		Authorization Bypass Through User-Controlled Key vulnerability in Apache InLong. This issue affects Apache InLong: from 1.4.0 through 1.8.0, some sensitive params checks will be bypassed, like			
		"autoDeserizalize", "allowLoadLocalInfile" . Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-			
		pick [1] to solve it.			
CVE-2023-43668	apache - inlong	[1] https://github.com/apache/inlong/pull/8604	2023-10-16	9.8	Critical
	oroglo zavikizila	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 unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability imposts). CVSS Vectors			
CVE-2023-22069	oracle - multiple products	Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-10-17	9.8	Critical
CVE-2023-22072	oracle - weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). The supported version	2023-10-17	9.8	Critical

		that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows			
		unauthenticated attacker with network access via T3, IIOP to			
		compromise Oracle WebLogic Server. Successful attacks of this			
		vulnerability can result in takeover of Oracle WebLogic Server.			
		CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability			
		impacts). CVSS Vector:			
		(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
		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 unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful			
		attacks of this vulnerability can result in takeover of Oracle			
		WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality,			
	oracle - multiple	Integrity and Availability impacts). CVSS Vector:			
CVE-2023-22089	products	(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-10-17	9.8	Critical
012 2020 22005	products	Unsafe Deserialization of User Input could lead to Execution of	2020 10 17	3.0	Or rerour
		Unauthorized Operations in Ivanti Endpoint Manager 2022 su3 and			
	ivanti - multiple	all previous versions, which could allow an attacker to execute			
CVE-2023-35084	products	commands remotely.	2023-10-18	9.8	Critical
	solarwinds -	The SolarWinds Access Rights Manager was susceptible to Remote			
	access_rights_man	Code Execution Vulnerability. This vulnerability can be abused by			
CVE-2023-35182	ager	unauthenticated users on SolarWinds ARM Server.	2023-10-19	9.8	Critical
		The SolarWinds Access Rights Manager was susceptible to Remote			
	solarwinds -	Code Execution Vulnerability. This vulnerability allows an			
	access_rights_man	unauthenticated user to abuse a SolarWinds service resulting in a			
CVE-2023-35184	ager	remote code execution.	2023-10-19	9.8	Critica
		The SolarWinds Access Rights Manager was susceptible to a			
	solarwinds -	Directory Traversal Remote Code Vulnerability. This vulnerability			
	access_rights_man	allows an unauthenticated user to achieve the Remote Code			
CVE-2023-35187	ager	Execution.	2023-10-19	9.8	Critical
		extract_user_to_sg in lib/scatterlist.c in the Linux kernel before			
		6.4.12 fails to unpin pages in a certain situation, as demonstrated			
CVE-2023-40791	linux - linux_kernel	by a WARNING for try_grab_page.	2023-10-16	9.1	Critical
		IBM Security Verify Privilege On-Premises 11.5 could allow a			
	ibm -	remote authenticated attacker to execute arbitrary commands on			
	security_verify_priv	the system by sending a specially crafted request. IBM X-Force ID:			
CVE-2022-22375	ilege_on-premises	221681.	2023-10-17	8.8	High
		Vulnerability in the Hospitality OPERA 5 Property Services product			
		of Oracle Hospitality Applications (component: Opera). The			
		supported version that is affected is 5.6. Easily exploitable			
		vulnerability allows low privileged attacker with network access via			
		HTTP to compromise Hospitality OPERA 5 Property Services.			
	oracle -	Successful attacks of this vulnerability can result in takeover of			
	hospitality_opera_	Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8			
0.45 2002 2005	hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector:	2022 40 47		
CVE-2023-22085	hospitality_opera_	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service s	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services.	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service s oracle -	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of	2023-10-17	8.8	High
CVE-2023-22085	hospitality_opera_ 5_property_service s oracle - hospitality_opera_	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8	2023-10-17	8.8	High
	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
	hospitality_opera_ 5_property_service s oracle - hospitality_opera_	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2023-10-17	8.8	High High
	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management			
CVE-2023-22087	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate	2023-10-17	8.8	High
CVE-2023-22087	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel.			
CVE-2023-22087	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds -	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote	2023-10-17	8.8	High
CVE-2023-22087 CVE-2023-41715	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows	2023-10-17	8.8	High High
CVE-2023-22085 CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds -	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API.	2023-10-17	8.8	High
CVE-2023-22087 CVE-2023-41715	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote	2023-10-17	8.8	High High
CVE-2023-22087 CVE-2023-41715	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds -	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an	2023-10-17	8.8	High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in	2023-10-17 2023-10-17 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds -	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution.	2023-10-17	8.8	High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect	2023-10-17 2023-10-17 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to	2023-10-17 2023-10-17 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect	2023-10-17 2023-10-17 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network.	2023-10-17 2023-10-17 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180 CVE-2023-35186	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man ager	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version:	2023-10-17 2023-10-19 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180 CVE-2023-35186	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later	2023-10-17 2023-10-17 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180 CVE-2023-35186	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man ager	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability ould allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later Vulnerability in the MySQL Connectors product of Oracle MySQL	2023-10-17 2023-10-19 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180 CVE-2023-35186	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man ager	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected	2023-10-17 2023-10-19 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180 CVE-2023-35186	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man ager	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.1.0 and prior. Difficult to exploit vulnerability allows	2023-10-17 2023-10-19 2023-10-19	8.8 8.8 8.8	High High High
CVE-2023-22087 CVE-2023-41715 CVE-2023-35180	hospitality_opera_ 5_property_service s oracle - hospitality_opera_ 5_property_service s sonicwall - sonicos solarwinds - access_rights_man ager solarwinds - access_rights_man ager	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected	2023-10-17 2023-10-19 2023-10-19	8.8 8.8 8.8	High High High

and while the vulnerability is in MySQL Connectors, statics may spiriterally impact deliboral product (Cocyo change). Successful attacks of this vulnerability are result in takepore of MySQL statics. A control of the vulnerability are result in takepore of MySQL statics. A control of the vulnerability in the Cocyo change. Successful vulnerability in the Cocyo was successful as a static static of the vulnerability of the Cocyo was successful. A control of the Cocyo vulnerability in the Cocyo was successful vulnerability and result in the source of oracle rushed was successful vulnerability allows unauthenderable state of the vulnerability can result in takeover of Oracle vulnerability allows unauthenderable state of the vulnerability and result in takeover of Oracle vulnerability allows unauthenderable state of the vulnerability in anomal. CVC Section 11, 121, 121, 121, 121, 121, 121, 121,	CVE-2023-22101	•	significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). 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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
attacks of this vulnerability, can result in takeover of MySQL Connectors, CSS 3.3 Base Score 8 (3 Kindhestality, Integrity and Availability impacts). CVSS vector. (VSS-3.1/AVAI/AG/MPSA/ULVS/SC)CLY/HI/AH). Vulnerability in the Oracle Velkalogis Server product of Oracle are afforced are 21.2.1.0 and 16.11.0.0 of filliotal to exploit vulnerability allows unautheristed statisker with network access vin 13.10 for componente Oracle Server and Velkogis Server. Server of Oracle Velkogis Server (VSS-3.1) Base Server (VSS-3.1) Base Server of Oracle Velkogis Server (VSS-3.1) Base Serve	CVE-2023-22101	•	attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). 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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
Comercion, CVSS 3.1 Rises Score 8.3 (Confidentially, Integrity and Availability impact). CVSS Vector: CVSS3.1/AVAIN_ACAI/PRANUER/SCC_FUN_IN_ACAI Vulnerability and the Drafted Vestocips Server products of Oracle rusion Middleware (component Core). Supported versions that a value and the Core of Core of Products of Core of Vestocips Server. Successful attacks of this vulnerability and result in Eakeware of Oracle Vestocips Server. Successful attacks of this vulnerability and result in Eakeware of Oracle Vestocips Server. Successful attacks of this vulnerability and the Server. Successful attacks of the Vestocips Server. Successful attacks of the Vestocips Server. Successful attacks of Vestocips Server. Successful attacks of the Vestocips Server. Successful attacks of this vulnerability is in MySGU, Installer. Successful attacks of this vulnerability is in MySGU, Installer. Successful attacks of this vulnerability is in MySGU, Installer. Successful attacks of this vulnerability is in MySGU, Installer. Successful attacks of this vulnerability and vestocips Server best of the Vestocips Server best Serv	CVE-2023-22101	•	Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). 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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
Availability impacts). CVSS vector: (CVS-32-32/WANG-MPNR-NULFS-CC-(H)-H/A-H). Volume-publishy in the Dracel Weblage, Server product of Oracle Human Middlewine (component Cond. Supported vectors to the are effected are 12.21.4.0 and 14.1.1.0.0 Direct to explore where the component Cond. Supported vectors to the are effected are 12.21.4.0 and 14.1.1.0.0 Direct to explore where the component Cond. volume State of the volume-public year and valuability impacts). CVSS vector: (CVF-2023-2790) produits. Volume-publity or the My20L installer product of Oracle My20L (CVF-2023-2790) produits. Volume-publity in the My20L installer product of Oracle My20L (CVF-2023-1290) produits. Volume-publity in the My20L installer product of Oracle My20L (CVF-2023-1290) produits. Volume-publity in the My20L installer product of Oracle My20L (CVF-2023-1290) produits. Volume-publity in the My20L installer product of Oracle My20L (CVF-2023-1290) produits where the control or the ministructure where My20L installer exceeds to components My20L installer. Successful attacks require human interaction from a person oracle than the attacker and while the volume-publity is in My20L installer. Successful attacks or the villengibility or installer. Successful attacks or the villengibility or installer. Successful attacks or the villengibility in product (scope change). Successful attacks or the villengibility in product (scope change). Successful attacks or the villengibility or installer. Volume-publity in the Oracle Will Villengibility or installer. Volume-publity in the Oracle Will Villengibility or installer. Volume-publity in the Oracle Will Villengibility or installer. Volume-publity in public oracle in Complete Oracle Will Villengibility impacts). Volume-publity in the Oracle Will Villengibility in public vil	CVE-2023-22101	•	Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). 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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
Vulnerability in the Oracle Verbicogic Server procuct of Oracle Fusion Middlework Component Coroc. Supported versions that are effected are 12.2.1.4.0 and 14.1.1.0.0 Difficult to exploit undershibty all control tackers with oracle vulnerability and result tacker with network access via 13,100 to compromise Oracle Medicing Server. Successful attacks of this vulnerability can result in tackers or Oracle products CVE 2023-22101 CVE 2023-22101 CVE 2023-22101 CVE 2023-22201 CVE 2023-22200	CVE-2023-22101	•	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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
Fusion Middleware (component. Core). Supported versions that are affected are 12.1.4.1.a.d mid. Li.l.D. Official to exploit value reability allows unautheriteated attacker with network access value attacks of this value reability and result in skeover of Oracle versions and the products of the value reability and result in skeover of Oracle versions and the products of the value reability and result in skeover of Oracle versions and the version of the value of Oracle versions and the versions of the value of Oracle versions and value of Oracle versions and value versions a	CVE-2023-22101	•	Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
are affected are 12,21,4,0 and 14,1,1,0,0 filliout to exploit vulnerability and sunarchard attacker with betwork access via TS, 10P to compromise Oracle Webblogic Server. Successful attacks of this vulnerability and certain in takeover of Oracle Webblogic Server. CVS3.3,17,0 Markability impacts; CVSS Vectors (CVSS-23,17,0 Markability) impacts; CVSS Vectors (CVSS-3,17,0 Markability) impacts; CVSS Vectors (CVSS-20,17,0 Markability) impacts; CVSS-20,17,0 Markability; CVSS-20,	CVE-2023-22101	•	are affected are 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
wincrability allows unauthenticated attacker with network access via Ta, IUP to compromise Drade weblog (severe, Successful attacks of this vulnerability can result in takeover of Oracle weblogs (severe, CVS 3.1 Base Sores 8.1 (confidentiality, Integrity and Availability impacts). CVSS vectors: (CVS-3073-7210) products Vinerability in the MySCI Installer product of Oracle MySCI (CVSS 3.1 AVAIVACHEPAN,UIN) (CVS) (CVS) Vectors: (CVSS 3.1 AVAIVACHEPAN,UIN) (CVS)	CVE-2023-22101	•	vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
via T3, 100-to compromise Oracle Weblage Server. Successful attacks of this windersbillity among value in takeover of the Vision Server. CVS3.3.1 Base Score 8.1 (confidentiality, integrity and Available) impacts. CVSS Vector: (CVS-3.3.1AV-3WA/CH/PR/MUNI/SUC-MP1/A/H). Vulnerability in the MySQL installer product of Oracle MySQL (comproment installer General). Supported versions that are officed are Profit of 1.0.8. Esily explorated versions that are officed or product of the MySQL Installer and the MySQL installer and the stacks require human interaction from a person other than the attacks rank while the vulnerability is in MySQL installer, stacks require human interaction from a person other than the attacks rank while the vulnerability is in MySQL installer, stacks require human interaction from a person other than the attacks rank while the vulnerability is in MySQL installer, stacks require human interaction from a person other than the attacks rank while the vulnerability is in MySQL installer, stacks require human interaction from a person other than the attacks rank while the vulnerability is in MySQL installer, stacks require human interaction from a person other than the attacks rank while the vulnerability is in MySQL installer, stacks required than an advantage of the person of the per	CVE-2023-22101	•	via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
attacks of this vulnerability can result in takeover of Oracle Weblogic Server, CVS 3.1 2800 score 3.1 (Confidentiality, Integrity and Availability imports), CVSS Vector: (CVS.53.1/AVAIACHEPR.VILVIALS/SCLVS) Vectors: (CVS.53.1/AVAIACHEPR.VILVIALS/SCLVS) Vectors: (CVS.53.1/AVAIACHEPR.VILVIALS/SCLVS) Vectors: (CVS.53.1/AVAIACHEPR.VILVIALS/SCLVS) Vectors: (CVS.53.1/AVAIACHEPR.VILVIALS/SCLVS) Vectors: (CVS.53.1/AVAIACHEPR.VILVIALS/SCLVS) Vectors: (CVS.53.1/AVAIACHEPR.VILVIALS Vectors) that are affected are Prior to 1.0.5. rasky exploitable vulnerability allows loop prolinged attacker with logor to the intrastructure where MySCL installer cencretals to compromise MySCL installer cencretals of the value of the Vilvial Vectors of the Vilvial Vector	CVE-2023-22101	•	attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
oracle - multiple Ove. 2023-22101 oracle - multiple products (CVS.33.1/AV.HA/C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.33.1/AV.HA/C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.33.1/AV.HA/C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.33.1/AV.HA/C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.33.1/AV.HA/C.H./PR.HVJU.H./S.LVC.H./H./H./H.). (CVS.33.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H./H.). (CVS.33.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.LVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.CVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.CVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.CVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.CVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.HVJU.H./S.CVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.H./H./H./S.CVC.H./H./H.). (CVS.30.1/AV.H./C.H./PR.H./H./H./H./L./PR.H./H./H./H./H./H./H./H./H./H./H./H./H./	CVE-2023-22101	•	WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
CVE-2023-32101 products (CVSS-3.1/ANN/ACH/PR-NyUN/S-U/C-H/H-H/A-H). 2023-10-17 8.1 High Values allow the component interest of the component interes	CVE-2023-22101	•	- , , , , ,	<u>'</u>		
Vulnerability in the MySQL installer of Conde MySQL (component installer: General). Supported versions that are affected are Prior to 1.6.8. Easily exploitable vulnerability allows tow privileged attacker with logn to the infrastructure where MySQL Installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability can result in unauthorized ability to cause a hang of requently repeatable crash (complete DOS) of MySQL Installer. Ander prepatable crash (complete DOS) of MySQL Installer. Note: This patch is used in MySQL Server bundled version 8.0.3 and 5.7.84. (VSS.3.1.3.1.2.4.7.C.M.PR.L.)MySQL.PQL. PR.L.)MySQL.PQL. PR.L., PQL. PQL. PQL. PQL. PQL. PQL. PQL. PQL.	CVE-2023-22101	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Components Installer, General). Supported versions that are affected are prior to 1.6. 8. Easily exploitable varientability allows low privileged attacker with logon to the infrastructure where NVySCI Installer executes to compromise MySCI Installer, stacker and while the unlarability is in MySCI Installer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability and mySCI Installer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability and result in unauthorized creation, deletion or modification access to critical data or all MySCI Installer cases being and another interest of the control of			, , , , , , , , , , , , , , , , , , , ,	2023-10-17	8.1	High
affected are Prior to 1.6.8. Easily exploitable vulnerability allows low privileged attacker with logn to the infrastructure where MySQL Installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability in in MySQL Installer, attacks and spiritually significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Installer. Note: This patch is used in MySQL Server bundled version 80.25 and 57.44. (VSS.3.1.8 ass Score 7.9 (Integrity and Availability impacts). CVSS Vector: OVF-2023-2094 oracle - mysql installer OVF-2023-2094 oracle - mysql installer OVF-2023-2095 oracle - mysql installer OVF-2023-2096 oracle - mysql installer OVF-2023-2097 oracle - mysql installer OVF-2023-2098 oracle - mysql installer OVF-2023-2098 oracle - mysql installer OVF-2023-2098 oracle - mysql installer OVF-2023-2099 oracle - mysql installer OVF-2023-2099 oracle - mysql installer OVF-2023-2090						
low privileged attacker with logon to the infrastructure where MySQL Installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Installer, attacks may significantly impact additional products (cope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Installer, attacks may significantly impact additional products (cope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Installer packs (complete DOS) of MySQL Installer packs (complete DOS) of MySQL Installer packs (complete DOS) of MySQL Installer. Vivos 3.1 Base Score 7.9 (Integrity and Availability impacts). CVSS 3.1 ANCL/ACL/PRI-I/UR/SC/C/WI-H/A-H). Vulnerability in the Oracle WM VirtualBox product of Oracle VM VirtualBox, attacks me Prior to 7.0.1.2 Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impacts). CVS 3.1 Base Score 7.9 (Integrity and Availability impacts). CVS 3.1 Base Score 7.9 (Integrity and Availability impacts). CVS 3.1 Base Score 7.9 (Integrity and Score) and CVS 3.1 Base Score 7.9 (Integrity and Score) and CVS 3.1 Base Score 7.9 (Integrity and Score) and CVS 3.1 Base Score 7.9 (Integrity and Score) and Score Score) and Score		·	, ,			
MySQL installer. Successful tracks require human interaction from a person other than the attacker and while the vulnerability is in MySQL installer, attacks may significantly impact additional products (scope change). Successful stracks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crants (complete DOS) of MySQL Installer. Nate: This patch is used in MySQL server bundled version 8.0.35 and 5.7.44. CVS.3.3.1 Base Score 7.9 (Integrity and Availability impacts). CVSS vector: (VE-2023-22004 mysql_installer VE-2023-22004 mysql_installer VE-2023-22100 mysql_instal			, ,			
than the attacker and while the vulnerability is in MySQL Installer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized death or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL installer. As a hang or frequently repeatable crash (complete DOS) of MySQL installer. With the county of the products of MySQL installer. With the county of MySQL installer. With the cou			, -			
attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL installer (VCE-2023-22094 mysql_installer) VEX.2023.22094 mysql_installer VEX.2023.22094 mysql_installer VIVIE-2023.22094 mysql_installer VIVIE-2023.22095 mysql_installer VIVIE-202			·			
cVE-2023-22094 mysq_installer cVE-2023-22095 mysq_installer cVE-2023-22095 mysq_installer cVE-2023-22095 mysq_installer cVE-2023-22095 mysq_installer cVE-2023-22095 mysq_installer cVE-2023-22096 mysq_installer			, , ,			
unauthorized creation, deletion or modification access to critical data or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Installer Note: This patch is used in MySQL Serve bundled version 8.0.35 and 5.7.44. CVSS.3.1 Base Score 7.9 (Integrity and Availability impacts). CVSS Vector (CVSS.3.1/AV:L/ACL/PR:L/U.R/S.C/C.N/H-I/A-H). Vulnerability in pacts (CVSS.3.1/AV:L/ACL/PR:L/U.R/S.C/C.N/H-I/A-H). Vulnerability in pacts (CVSS.3.1/AV:L/ACL/PR:L/U.R/S.C/C.N/H-I/A-H). Vulnerability in the Oracle V MirtualBox product of Oracle VirtualBox in the Oracle V MirtualBox in the Oracle V Mir			, , , , , , , , , , , , , , , , , , , ,			
data or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete POS)s of MySQL Installer. Note: This patch is used in MySQL Server bundled version 8.0.35 and 57.44 CVS 3.1 Base Score 7.9 (Integrity and Availability impacts), CVSS Vector: (VES.23.1/AV:1/ACCL/PR:L/UR.S/S/C/DN:H/H/A:H). Volunerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12 Easily exploitable vulnerability allows high privileged datacker with logon to the infrastructure where Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. While the vulnerability van proplete access to all Oracle VM VirtualBox. While the vulnerability van proplete access to all Oracle VM VirtualBox and proplete access to all Oracle VM VirtualBox and proplete access to all Oracle VM VirtualBox Note: Only applicable to 7.0x platform. OVE 3.1 Base Score 7.9 (Confidentially and Availability impacts). CVSS Vector: (CVSS.3.1 JAVL/ACL/PR:H/UIN/SC/C-I/JN/AH). BM Directory Server for IBM I contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privilege sto gain component access to the host operating system. IBM Force ID: 263584. BM High EVE-2023-40377 products BM Fige VE-2023-40378 products ibm - multiple or an elevate privilege to gain component access to the host operating system. IBM X-Force ID: 263584. BM High Clark Command line access to the host operating system. IBM X-Force ID: 263584. BM High Clark Command In access to the host operating system. IBM X-Force ID: 263584. BM High Clark Command In access to the host operating system. IBM X-Force ID: 260740. The Linux kernel before S-5 has an act use after-f						
to cause a hang or frequently repeatable crash (complete DOS) of MySQL Installer. Note: This patch is used in MySQL Server bundled version 8.0.35 and 5.7.44. CVSS 3.1 Base Score 7.9 (Integrity and Availability imparts). CVSS Vector. (CVSS.33.1/AV-I_ACA:1/PR-II/UR-II/SC/C-N/ISH/ACH). (CVS-2023-22004 mysql_installer			·			
wysQL installer. Note: This patch is used in MySQL server bundled version 8.0 3s and 5.74. CVSS 14 best Score 7.9 (Integrity and Availability impacts). CVSS Vector: (VSS-3.1/AV:1/AC:1/PR:H/U.IR/SC/C.M/H-I/A:H). Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. Note: Only applicable to 7.0 x. platform. Oracle VM VirtualBox. Note: Only applicable to 7.0 x. platform. Oval 2.1 asses Score 7.9 (Confidentality impacts). CVE-2023-22100 vm virtualbox Vm virtualBox. VirtualBox. Note: Only applicable to 7.0 x. platform. IBM Directory Server for IBM I contains a local privilege scalation vulnerability. A malicious actor with command line access to the host operating system. IBM X-Force ID: 263583. Backup, Recovery, and Media Services (RBMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with component access to the host operating system. IBM X-Force ID: 263583. OVE-2023-40377 products ibm - multiple system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. 2023-10-15 7.8 High malicious actor with command line access to the host operating system. IBM X-Force ID: 263583. 1023-10-16 7.8 High malicious actor with component access to the host operating system. IBM X-Force ID: 263583. 1023-10-16 7.8 High malicious access on a restricted shell. IBM X-Force ID: 263583. 1023-10-16 7.8 High malicious access on a restricted shell. IBM X-For			·			
oracle- mysql_installer ("CVS-33_AVX-1/AC-L/PR-R/U-IR/SC-(N/H-I/A-H-I). Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. Note: Only applicable to 7.0 x platform. CVF-2023-22100 vm virtualbox CVE-2023-40378 products Dm - multiple products D						
CVE-2023-22094 mysql_installer			version 8.0.35 and 5.7.44. CVSS 3.1 Base Score 7.9 (Integrity and			
Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. Note: Only applicable to 7.0. pathorm. CVS-2023-22100 Oracle - VM VirtualBox. Note: Only applicable to 7.0. pathorm. CVS-3.1 Base Score 7.9 (Confidentiality and Availability impacts). CVF-2023-22100 Vm_virtualbox. VS Sector: (CVS-3.1/AVI-I/ACI-I/PRI-I/INI/NS-I/I-I). IBM Directory Server for IBM I contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privileges to gain component access to the host operating system and levate privileges to gain component access in the not operating system and levate privileges to gain component access in the not operating system in the command line access to the host operating system in the command line access to the host operating system in the command line access to the host operating system in the command line access to the products Dibm - multiple products Dibm			, , ,			
Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability; allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox. While the vulnerability; is in Gracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successif but attacks of this vulnerability; can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0 x platform. CVE-2023-22100 vm_virtualbox CVS 3.1 Base Score 7.9 (Considentiality and Availability impacts). CVS Svector: (CVS.3.1/AV:1/AC:1/PR:H/U.IN/S:C/CHI/EN/A-IH). IBM Directory Server for IBM I contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-force ID: 263584. 2023-10-15 7.8 High Dibm - multiple products access in the host operating system. IBM X-force ID: 263584. 2023-10-16 7.8 High EVE-2023-40377 products brown and the access to the host operating system and evaluer privileges to gain component access to the host operating system and privileges calation vulnerability. A malicious actor with command line access to the host operating system and the privileges to gain component access to the host operating system and privilege scalation vulnerability. A malicious actor with command line access to the host operating system and privilege scalation vulnerability. A malicious actor with command line access to the host operating system and privilege scalation vulnerability. This vulnerability allows accessing the privilege scalation vulnerability. This vulnerability allows accessing the privilege scalation vulnerability. This vulnerability allows accessing the privilege scalation vulnerability. This vulnerability allow	CVE-2023-22094	mysql_installer		2023-10-17	7.9	High
affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged stacker with logon to the infrastructure where Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. Accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete OOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0 x platform. CVE-2023-22100 vm virtualbox CVE-2023-22100 vm virtualbox CVSS Vector: (CVSS-3.1/AV-1/ACL/PR-I/MI-MS-I/C-I/MI-MI-M) ibm - multiple ibm - multiple cVE-2023-40378 products ibm - multiple ibm - multiple ibm - multiple ibm - multiple cVE-2023-40377 products products brandling and availability. A middlous actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263584. 2023-10-15 7.8 High CVE-2023-40377 products cVE-2023-40377 products brandling and access to the host operating system. IBM X-Force ID: 263583. 2023-10-16 7.8 High CVE-2023-38280 products cVE-2023-38280						
high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVE-2023-22100 vm_virtualbox. CVSS 3.1 Base Score 7.9 (Confidentiality and Availability impacts). CVS Vector: (CVSS.3.1/AV:L/AC:L/PR:H/UINS:CC-H/ENA/A:H). BIBM Directory Server for IBM i contains a local privilege ascalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263584. Backup, Recovery, and Media Services (BRMS) for IBM 17.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system an elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. Diminus - Innux -						
Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. Note: Only applicable to 7.0.x platform. Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVE-2023-22100 vm_virtualBox Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.9 (Confidentiality and Availability impacts). IBM Directory Server for IBM i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privilege sto gain component access to the host operating system. IBM X-Force ID: 263584. Backup, Recovery, and Media Services (BRMIS) for IBM 17.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system is malicious actor with command line access to the host operating system. IBM X-Force ID: 263584. Solarivinds A malicious actor with command line access to the host operating system. IBM X-Force ID: 263585. 10x			, ,			
VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to change). Successful attacks of this vulnerability can result in unauthorized access to change). Successful adds and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0x. platform. CVE-2023-22100 vm_virtualBox. CVES Vector: (CVSS.3.1/AV:1/AC:1/PR:H/VIIN/S:C/C-H/I:N/A:H). Dibm - multiple wiln - multiple host operating system can elevate privileges to gain component access to the host operating system. BM X-force ID: 263584. Dibm - multiple system can elevate privilege scalation vulnerability. A malicious actor with command line access to the host operating system. BM X-force ID: 263584. Dibm - multiple system and elevate privileges to gain component access to the host operating system. BM X-force ID: 263584. Dibm - multiple system and elevate privileges to gain component access to the host operating system and elevate privileges to gain component access to the host operating system. BM X-force ID: 263584. Dibm - multiple system and elevate privileges to gain component access to the host operating system and elevate privileges to gain component access to the host operating system. BM X-force ID: 263583. Dibm - multiple system and elevate privileges to gain component access to the host operating system. BM X-force ID: 263583. Dibm - multiple system and elevate privileges to gain component access to the host operating system. BM X-force ID: 263583. Dibm - multiple system and elevate privileges to gain component access to the host operating system. BM X-force ID: 260740. Dibm - multiple system and elevate privileges to control to the system and elevate privilege status. Privilege Scalation. Dibm - multiple system and elevate privilege status or elevate privilege status. Privilege Scalation. Dibm - multiple system			• . •			
change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0 x platform. oracle - CVSS 3.1 Base Score 7.9 (Confidentiality and Availability impacts). vm virtualbox CVSS Vector: (CVSS.3.1/AVI./ACI./PR:H/UI:N/S.C/C.H/IN-IA:H). Bib Tib Tib VirtualBox Note: Only applicable to 7.0 x platform. CVSS Vector: (CVSS.3.1/AVI./ACI./PR:H/UI:N/S.C/C.H/IN-IA:H). IBM Directory Server for IBM i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privilege scalation vulnerability. A malicious actor with command line access to the host operating system. IBM X-Force ID: 263584. CVE-2023-40377 products products products products products privilege sto gain component access to the host operating system. IBM X-Force ID: 263583. CVE-2023-38280 products pro			VirtualBox. While the vulnerability is in Oracle VM VirtualBox,			
unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0 x platform. CVSS 3.1 Base Score 7.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:H). IBM Directory Server for IBM i contains a local privilege escalation unlerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privilege sto gain component access to the host operating system can elevate privilege sto gain component access to the host operating system. IBM X-Force ID: 263584. Backup, Recovery, and Media Services (BRNS) for IBM 17.2, 7.3, and 7.4 contains a local privilege scalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.103.0.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. CVE-2023-38280 Iniux - linux kernel solarwinds - access_rights_man ager The Linux kernel before 6.5.4 has an est use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent. 2023-10-16 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this			, , , , , , , , , , , , , , , , , , , ,			
Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVES 2023-22100 vm_virtualbox CVES 3.1 Base Score 7.9 (Confidentiality and Availability impacts). IBM Directory Server for IBM i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system. CVES 2023-40378 Description of the first virtual box or virtual box			• .			
cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVE3.18 ass Score 7.9 (Confidentiality and Availability Impacts). CVS3.18 ass Score 7.9 (Confidentiality Impacts). CVE-2023-40378 Impact Score 7.9 (Confidentiality Impacts). CVE-2023-40379 Impact Score 7.9 (Confidentiality			·			
oracle - vm_virtualbox			,			
oracle - Vm_virtualbox			• , , , , , , , , , , , , , , , , , , ,			
CVE-2023-22100 vm_virtualbox CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:H). 2023-10-17 7.9 High lBM Directory Server for IBM i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263584. 2023-10-15 7.8 High Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-force ID: 263584. 2023-10-15 7.8 High Ibm - multiple products products products products products products products products lBM X-Force ID: 263583. 2023-10-16 7.8 High Ibm - multiple products produ		oracle -				
vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263584. Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the story operating system. IBM X-Force ID: 263584. EVE-2023-40377 products produc	CVE-2023-22100		• • • • • • • • • • • • • • • • • • • •	2023-10-17	7.9	High
ibm - multiple products access to the host operating system. IBM X-Force ID: 263584. Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system. IBM X-Force ID: 263583. Ibm - multiple products pro			, , ,			
Backup, Recovery, and Media Services (BRMS) for IBM 1-7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privilege to gain component access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privileges to gain component access to the host operating system. IBM M-K-orce ID: 263583. IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. CVE-2023-38280		10.	•			
Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. 2023-10-16 7.8 High IBM Tender of IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. 2023-10-16 7.8 High IBM X-Force ID: 260740. The Linux kernel before 6.5.4 has an est use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent. 2023-10-16 7.8 High IBM X-Force ID: 260740. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. 2023-10-19 7.8 High IBM X-Force ID: 260740. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. 2023-10-19 7.8 High IBM X-Force ID: 260740. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. 2023-10-19 7.8 High IBM X-Force ID: 260740. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. 2023-10-19 7.8 High IBM X-Force ID: 260740. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. 2023-10-19 7.8 High IBM X-Force ID: 260740. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability This vulnerability allows authenticated users to abuse local resources to Privilege escalation Vulnerability allows authenticated users to abuse local resources to Privilege escalation Vulnerability allows au	CVE 2022 40270	•		2022 10 15	7.0	امان ال
and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. 2023-10-16 7.8 High IBM - multiple products products IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. 2023-10-16 7.8 High The Linux kernel before 6.5.4 has an est use-after-free in Sext4/extents_status.c, related to ext4_es_insert_extent. 2023-10-16 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to a access_rights_man ager abuse incorrect folder permission resulting in Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation Vulnerability allows authenticated users to abuse local resources to Privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system	CVE-2023-403/8	products		2023-10-15	۷.۷	нıgn
malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. IBM HMC (Hardware Management Console) 10.1.1010.0 and ibm - multiple products 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. 2023-10-16 7.8 High			• • • • • • • • • • • • • • • • • • • •			
ibm - multiple products both one of the host operating system. IBM X-Force ID: 263583. 2023-10-16 7.8 High ibm - multiple products products ibm - multiple products p			, -			
Description		ibm - multiple	, -			
IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. 2023-10-16 7.8 High	CVE-2023-40377	·		2023-10-16	7.8	High
CVE-2023-38280 products root access on a restricted shell. IBM X-Force ID: 260740. 2023-10-16 7.8 High The Linux kernel before 6.5.4 has an es1 use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent. 2023-10-16 7.8 High Solarwinds - access_rights_man ager access_rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. 2023-10-19 7.8 High CVE-2023-35183 ager Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. 2023-10-19 7.8 High VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system			IBM HMC (Hardware Management Console) 10.1.1010.0 and			
The Linux kernel before 6.5.4 has an es1 use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent. Solarwinds - access_rights_man ager CVE-2023-35181 ager The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. The SolarWinds Access Rights Wanager was susceptible to Privilege Escalation. The SolarWin		•	, -	_		
CVE-2023-45898 linux - linux_kernel fs/ext4/extents_status.c, related to ext4_es_insert_extent. 2023-10-16 7.8 High solarwinds - access_rights_man ager Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. 2023-10-19 7.8 High Solarwinds - access_rights_man access_rights_man ager Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. 2023-10-19 7.8 High VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system	CVE-2023-38280	products		2023-10-16	7.8	High
solarwinds - access_rights_man ager	CVE 2022 45000	linuv linuv linuv linuv		2022 10 10	7.0	ماہ :۱۱
access_rights_man ager Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows access_rights_man ager CVE-2023-35183 Ager VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system Privilege Escalation. 2023-10-19 7.8 High This Vulnerability allows users to abuse local resolution. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. Privilege Escalation. Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. Privilege Escalation. Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. Privilege Escalation. Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation. Privilege Es	<u>CVE-2U23-45898</u>	_		2023-10-16	7.8	High
CVE-2023-35181 ager abuse incorrect folder permission resulting in Privilege Escalation. 2023-10-19 7.8 High The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. CVE-2023-35183 ager Escalation. VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system	1		,			
The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system			•	2023-10-19	7.8	High
solarwinds - access_rights_man ager CVE-2023-35183 Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation. VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege 2023-10-19 7.8 High						
CVE-2023-35183 ager Escalation. VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system		solarwinds -	,			
VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system		access_rights_man	authenticated users to abuse local resources to Privilege			
escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system	CVE-2023-35183	ager		2023-10-19	7.8	High
installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system						
application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system			,	,		
an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system			• • • • • • • • • • • • • • • • • • • •			
upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system						
privileges may exploit this vulnerability to escalate privileges to root on the system						
system						
			, , ,			
national contractions and the contraction of the co	0) (5, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0		·	0000		
	CVE-2023-34045	vmware - fusion	where Fusion is installed or being installed for the first time.	2023-10-20	7.8	High
Improper Neutralization of Special Elements used in an SQL			·			
Command ('SQL Injection') vulnerability in Apache InLong. This CVE-2023-43667 apache - inlong issue affects Apache InLong: from 1.4.0 through 1.8.0, the attacker 2023-10-16 7.5 High	CVF-2023-42667	anache - inlong	, , ,	2023-10-16	75	High

	T		Г	I I	
		can create misleading or false records, making it harder to audit			
		and trace malicious activities. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick [1] to solve it.			
		Apacite intolig 3 1.0.0 of cherry pick [1] to solve it.			
		[1] https://github.com/apache/inlong/pull/8628			
		Grafana is an open-source platform for monitoring and			
		observability.			
		The Google Sheets data source plugin for Grafana, versions 0.9.0			
		to 1.2.2 are vulnerable to an information disclosure vulnerability.			
		The plugin did not properly sanitize error messages, making it			
		potentially expose the Google Sheet API-key that is configured for			
		the data source.			
	grafana -				
CVE-2023-4457	google_sheets	This vulnerability was fixed in version 1.2.2.	2023-10-16	7.5	High
		IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
		Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a			
CVE 2022 20007	ibm - multiple	specially crafted query on certain databases. IBM X-Force ID:	2022 10 16	7.5	مات ۱۱:
CVE-2023-30987	products	253440. IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect	2023-10-16	7.5	High
		Server) 11.5 and 11.5 is vulnerable to denial of service with a			
	ibm - multiple	specially crafted ALTER TABLE statement. IBM X-Force ID:			
CVE-2023-38720	products	261616.	2023-10-16	7.5	High
	·	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
	ibm - multiple	Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a			
CVE-2023-38728	products	specially crafted XML query statement. IBM X-Force ID: 262258.	2023-10-16	7.5	High
		IBM Db2 for Linux, UNIX, and Windows (includes Db2 Connect			
		Server) 11.5 is vulnerable to a denial of service with a specially			
CVE-2023-38740	ibm - db2	crafted SQL statement. IBM X-Force ID: 262613.	2023-10-16	7.5	High
	there are the la	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
CVE-2023-30991	ibm - multiple products	Server) 11.1 and 11.5 is vulnerable to denial of service with a	2023-10-16	7.5	⊔iαh
CVE-2023-30991	products	specially crafted query. IBM X-Force ID: 254037. IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect	2023-10-16	7.5	High
		Server) 11.5 is vulnerable to denial of service with a specially			
CVE-2023-40374	ibm - db2	crafted query statement. IBM X-Force ID: 263575.	2023-10-16	7.5	High
<u> </u>		IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect		7.10	6
		Server) 11.5 is vulnerable to denial of service with a specially			
		crafted SQL statement using External Tables. IBM X-Force ID:			
CVE-2023-40372	ibm - db2	263499.	2023-10-17	7.5	High
		IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
	26 102 . 1 .	Server) is vulnerable to denial of service with a specially crafted			
CVE-2023-40373	ibm - multiple products	query containing common table expressions. IBM X-Force ID: 263574.	2023-10-17	7.5	⊔iah
CVE-2023-40373	products	203374.	2023-10-17	7.5	High
	ibm -	IBM Security Verify Privilege On-Premises 11.5 could disclose			
	security_verify_priv	sensitive information to an attacked due to the transmission of			
CVE-2022-22385	ilege_on-premises	data in clear text. IBM X-Force ID: 221962.	2023-10-17	7.5	High
		Improper Input Validation vulnerability in Apache Traffic Server			
		with malformed HTTP/2 frames. This issue affects Apache Traffic			
		Server: from 9.0.0 through 9.2.2.			
0.45 2022 2045	apache -	Users are recommended to upgrade to version 9.2.3, which fixes	2022 40 47	- -	
CVE-2023-39456	traffic_server	the issue.	2023-10-17	7.5	High
		Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Traffic Server. This issue affects Apache			
		Traffic Server: from 8.0.0 through 8.1.8, from 9.0.0 through 9.2.2.			
		Traine Server. Home close through cline, from 5.0.0 through 5.2.2.			
	apache - multiple	Users are recommended to upgrade to version 8.1.9 or 9.2.3,			
CVE-2023-41752	products	which fixes the issue.	2023-10-17	7.5	High
		Vulnerability in the Oracle HTTP Server product of Oracle Fusion			
		Middleware (component: Web Listener). The supported version			
		that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows			
		unauthenticated attacker with network access via HTTP to			
		compromise Oracle HTTP Server. Successful attacks of this			
		vulnerability can result in unauthorized access to critical data or			
		complete access to all Oracle HTTP Server accessible data. CVSS			
CVE-2023-22019	oracle - http_server	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).	2023-10-17	7.5	High
CVL-2023-22019	oracie - nttp_server	Vulnerability in the Oracle WebLogic Server product of Oracle	2023-10-1/	1.5	ıııgıı
		Fusion Middleware (component: Core). Supported versions that			
		are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable			
	i .	vulnerability allows unauthenticated attacker with network access			
		vallerability allows allautheriticated attacker with network access			
		via T3, IIOP to compromise Oracle WebLogic Server. Successful			
		via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to			
		via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server			
CVE-2023-22086	oracle - multiple products	via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to	2023-10-17	7.5	High

		William hilling in the Orgale Weblack Construction (CO.)		ı	
		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 unauthenticated attacker with network access			
		via T3, IIOP to compromise Oracle WebLogic Server. Successful			
		attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server			
	oracle - multiple	accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts).			
CVE-2023-22108	products	CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-10-17	7.5	High
		SonicOS Use of Hard-coded Password vulnerability in the			
CVE-2023-41713	sonicwall - sonicos	'dynHandleBuyToolbar' demo function. A password disclosure vulnerability in the Secure PDF eXchange	2023-10-17	7.5	High
		(SPX) feature allows attackers with full email access to decrypt			
		PDFs in Sophos Firewall version 19.5 MR3 (19.5.3) and older, if the			
CVE-2023-5552	sophos - firewall	password type is set to "Specified by sender".	2023-10-18	7.5	High
		In multiple functions of protocolembmsadapter.cpp, there is a			
		possible out			
		of bounds read due to a missing bounds check. This could lead to remote			
		information disclosure with no additional execution privileges			
		needed. User			
CVE-2023-35656	google - android	interaction is not needed for exploitation.	2023-10-18	7.5	High
		In Init of protocolnetadapter.cpp, there is a possible out of bounds read			
		due to a missing bounds check. This could lead to remote			
		information			
		disclosure with no additional execution privileges needed. User			
C) /F 2222 2777		interaction	2020 15 15		
CVE-2023-35663	google - android	is not needed for exploitation.	2023-10-18	7.5	High
		Deserialization of Untrusted Data Vulnerability in Apache Software			
		Foundation Apache InLong.			
		This issue affects Apache InLong: from 1.4.0 through 1.8.0, the			
		attacker can use \t to bypass. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it.			
		Apacite intering 3 1.3.0 or energy pick [1] to solve it.			
CVE-2023-46227	apache - inlong	[1] https://github.com/apache/inlong/pull/8814	2023-10-19	7.5	High
		Vulnerability in the Oracle VM VirtualBox product of Oracle			
		Virtualization (component: Core). Supported versions that are			
		affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where			
		Oracle VM VirtualBox executes to compromise Oracle VM			
		VirtualBox. While the vulnerability is in Oracle VM VirtualBox,			
		attacks may significantly impact additional products (scope			
		change). Successful attacks of this vulnerability can result in			
		unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as			
		unauthorized update, insert or delete access to some of Oracle VM			
		VirtualBox accessible data and unauthorized read access to a			
		subset of Oracle VM VirtualBox accessible data. Note: Only			
	oracle -	applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3			
CVE-2023-22098	oracie - vm_virtualbox	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2023-10-17	7.3	High
		Vulnerability in the Oracle VM VirtualBox product of Oracle			۰۰۰۵۰۰
		Virtualization (component: Core). Supported versions that are			
		affected are Prior to 7.0.12. Easily exploitable vulnerability allows			
		high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM			
		VirtualBox. While the vulnerability is in Oracle VM VirtualBox,			
		attacks may significantly impact additional products (scope			
		change). Successful attacks of this vulnerability can result in			
		unauthorized ability to cause a hang or frequently repeatable			
		crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM			
		• •			
		VirtualBox accessible data and unauthorized read access to a			
		VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Only			
		subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3			
CVE 2022 22000	oracle -	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	2022 40 47	7.3	مان≕ا۔
CVE-2023-22099	vm_virtualbox	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2023-10-17	7.3	High
CVE-2023-22099	vm_virtualbox ibm -	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). IBM Security Verify Governance 10.0 could allow a privileged use	2023-10-17	7.3	High
CVE-2023-22099 CVE-2023-35018	vm_virtualbox	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2023-10-17	7.3	High High
	vm_virtualbox ibm - security_verify_gov	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382. Grafana is an open-source platform for monitoring and			
	vm_virtualbox ibm - security_verify_gov	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382. Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with			
	vm_virtualbox ibm - security_verify_gov	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382. Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a user with Organization Admin			
	vm_virtualbox ibm - security_verify_gov	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382. Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with			-
	vm_virtualbox ibm - security_verify_gov	subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382. Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a user with Organization Admin permissions in one organization to change the permissions			-

It also allows an Organization Admin to assign or revoke any permissions that they have to any user globally. This means that any Organization Admin can elevate their own permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of. Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. We grafana - multiple products of the characters in the request address. 2023-10-17 7.2	High
permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of. Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. grafana - multiple However, the restriction can be bypassed used punycode encoding	High
organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of. Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. grafana - multiple However, the restriction can be bypassed used punycode encoding	High
In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. grafana - multiple However, the restriction can be bypassed used punycode encoding	High
	High
CVE-2023-4399 products of the characters in the request address. 2023-10-17 7.2 solarwinds - access_rights_man The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability using SYSTEM Directory Traversal Remote Code Vulnerability using SYSTEM	
<u>CVE-2023-35185</u> ager privileges. 2023-10-19 7.2	High
IBM Security Verify Privilege On-Premise 11.5 could allow an authenticated user to obtain sensitive information or perform unauthorized actions due to improper input validation. IBM X- CVE-2021-29913 ilege_on-premises Force ID: 207898. 2023-10-17 7.1	High
VMware Fusion(13.x prior to 13.5) contains a TOCTOU (Time-of-check Time-of-use)	
vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg'	
volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system	
CVE-2023-34046 vmware - fusion where Fusion is installed or being installed for the first time. 2023-10-20 7	High
Insufficient Verification of Data Authenticity vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0,	
General user can view all user data like Admin account. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-	
pick [1] to solve it.	
CVE-2023-43666apache - inlong[1] https://github.com/apache/inlong/pull/86232023-10-166.5A vulnerability exists which allows an authenticated attacker to	Medium
access sensitive information on the AirWave Management Platform web-based management interface. Successful exploitation allows the attacker to gain access to some data that could be further exploited to laterally access devices managed and multiple products monitored by the AirWave server. 2023-10-17 6.5	Medium
Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable 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 oracle - multiple MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS	Medium
Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable 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. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector:	
CVE-2023-22079 oracle - mysql (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). 2023-10-17 6.5 Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Events & Notifications). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CC	Medium
ise_cost_center_co	
	Medium

		,		1	1
		Application Objects 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).			
		Vulnerability in the Oracle iRecruitment product of Oracle E-			
		Business Suite (component: Requisition and Vacancy). 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 iRecruitment. Successful attacks			
		of this vulnerability can result in unauthorized update, insert or			
		delete access to some of Oracle iRecruitment accessible data as			
		well as unauthorized read access to a subset of Oracle			
		iRecruitment accessible data. CVSS 3.1 Base Score 6.5			
	oracle - e-	(Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22093	business_suite	(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2023-10-17	6.5	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). The supported version that is			
		affected is 8.1.0. Easily exploitable 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. CVSS 3.1 Base			
		Score 6.5 (Availability impacts). CVSS Vector:			
CVE-2023-22095	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	6.5	Medium
		Vulnerability in the Oracle Enterprise Command Center			
		Framework product of Oracle E-Business Suite (component: API).			
		Supported versions that are affected are ECC: 8, 9 and 10. Easily			
		exploitable vulnerability allows low privileged attacker with			
		network access via HTTP to compromise Oracle Enterprise			
		Command Center Framework. Successful attacks of this			
		vulnerability can result in unauthorized access to critical data or			
		complete access to all Oracle Enterprise Command Center			
		Framework accessible data. CVSS 3.1 Base Score 6.5			
	oracle - multiple	(Confidentiality impacts). CVSS Vector:			
CVE-2023-22106	products	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2023-10-17	6.5	Medium
		Vulnerability in the Oracle FLEXCUBE Universal Banking product of			
		Oracle Financial Services Applications (component: Infrastructure).			
		Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and			
		14.5-14.7. Easily exploitable vulnerability allows low privileged			
		attacker with network access via HTTP to compromise Oracle			
		FLEXCUBE Universal Banking. Successful attacks require human			
		interaction from a person other than the attacker and while the			
		vulnerability is in Oracle FLEXCUBE Universal Banking, 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 FLEXCUBE Universal			
		Banking accessible data as well as unauthorized read access to a			
		subset of Oracle FLEXCUBE Universal Banking accessible data and			
		unauthorized ability to cause a partial denial of service (partial			
		DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score			
CVE 2022 22440	oracle - multiple	6.5 (Confidentiality, Integrity and Availability impacts). CVSS	2022 40 47	6.5	N A a aliana
CVE-2023-22118	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).	2023-10-17	6.5	Medium
		ConicOC nost authoration stack board buffer and file			
		SonicOS post-authentication stack-based buffer overflow			
		vulnerability in the getBookmarkList.json URL endpoint leads to a			
CVE 2022 2027C	conjected as the	firewall crash.	2022 40 47		NA selie ee
CVE-2023-39276	sonicwall - sonicos		2023-10-17	6.5	Medium
		ConicOC nest outhantication start beautiful Conic			
		SonicOS post-authentication stack-based buffer overflow			
CVE 2022 2027	conicuall conica	vulnerability in the sonicflow.csv and appflowsessions.csv URL	2022 40 47	6.5	NAcal:
CVE-2023-39277	sonicwall - sonicos	endpoints leads to a firewall crash.	2023-10-17	6.5	Medium
		SonicOS post-authentication user assertion failure leads to Stack-			
CVE 2022 20270	conjournil	Based Buffer Overflow vulnerability via main.cgi leads to a firewall	2022 40 47	C -	N 4 c al !
CVE-2023-39278	sonicwall - sonicos	crash.	2023-10-17	6.5	Medium
		SonicOS post-authentication Stack-Based Buffer Overflow			
CVE 2022 20270	conjewall coniect	vulnerability in the getPacketReplayData.json URL endpoint leads	2022 40 47	6.5	Madium
CVE-2023-39279	sonicwall - sonicos		2023-10-17	6.5	Medium
		SonicOS p			
		ost-authentication Stack-Based Buffer Overflow vulnerability in the			
		ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall			
CVE-2023-39280	sonicwall - sonicos	crash.	2023-10-17	6.5	Medium
<u> </u>	SOTTICEVEGIT SOTTICUS	SonicOS post-authentication Stack-Based Buffer Overflow	_U_U_1/	0.5	ivicululli
		Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to			
CVE-2023-41711	sonicwall - sonicos	a firewall crash.	2023-10-17	6.5	Medium
CAT 5052-41/11	Joinewan - Suilleus	SonicOS post-authentication Stack-Based Buffer Overflow	~0~J-10-1/	0.5	ivicululli
		Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a			
CVE-2023-41712	sonicwall - sonicos	firewall crash.	2023-10-17	6.5	Medium
CVL-2U23-41/12	ivanti - multiple	Allows an authenticated attacker with network access to read	ZUZ3-1U-1/	0.5	ivicululli
CVE-2023-35083	products	arbitrary files on Endpoint Manager recently discovered on 2022	2023-10-18	6.5	Medium
CVL ZUZJ-JJU03	ρισαάτιδ	arbitrary mes on Enapoint Manager recently discovered on 2022	7077-10-10	0.5	ivicululli

Г		SU3 and all previous versions potentially leading to the leakage of			
		sold and all previous versions potentially leading to the leakage of sensitive information.			
		A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager			
		could allow an authenticated, remote attacker to retrieve arbitrary			
		files from an affected system.			
		This vulnerability is due to improper validation of parameters that			
		are sent to the web UI. An attacker could exploit this vulnerability			
		by logging in to Cisco Catalyst SD-WAN Manager and issuing			
		crafted requests using the web UI. A successful exploit could allow			
	cisco - multiple	the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the			
CVE-2023-20261	products	attacker must be an authenticated user.	2023-10-18	6.5	Medium
	p. o alone				
		There exists an SSRF (Server-Side Request Forgery) vulnerability			
		located at the /sandbox/proxyGateway endpoint. This vulnerability			
		allows us to manipulate arbitrary requests and retrieve corresponding responses by inputting any URL into the requestUrl			
		parameter.			
		Of particular concern is our ability to exert control over the HTTP			
		method, cookies, IP address, and headers. This effectively grants us the capability to dispatch complete HTTP requests to hosts of			
		our choosing.			
		This issue affects Apache ShenYu: 2.5.1.			
		Upgrade to Apache ShenYu 2.6.0 or apply			
CVE-2023-25753	apache - shenyu	patch https://github.com/apache/shenyu/pull/4776 .	2023-10-19	6.5	Medium
		All versions of Apache Santuario - XML Security for Java prior to			
		2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable			
		to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is			
	apache - multiple	enabled. Users are recommended to upgrade to version 2.2.6,			
CVE-2023-44483	products	2.3.4, or 3.0.3, which fixes this issue.	2023-10-20	6.5	Medium
		Vulnerability in the Oracle Outside In Technology product of			
		Oracle Fusion Middleware (component: Content Access SDK, Image Export SDK, PDF Export SDK, HTML Export SDK). The			
		supported version that is affected is 8.5.6. Easily exploitable			
		vulnerability allows low privileged attacker with network access via			
		HTTP to compromise Oracle Outside In Technology. Successful			
		attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology			
		accessible data as well as unauthorized read access to a subset of			
		Oracle Outside In Technology accessible data and unauthorized			
	مادماد	ability to cause a partial denial of service (partial DOS) of Oracle			
	oracle - outside_in_technol	Outside In Technology. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
CVE-2023-22127	ogy	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2023-10-17	6.3	Medium
		Security vulnerability in Apache bRPC <=1.6.0 on all platforms		_	
		allows attackers to inject XSS code to the builtin rpcz page.			
		An attacker that can send http request to bRPC server with rpcz enabled can inject arbitrary XSS code to the builtin rpcz page.			
		The same of the sa			
		Solution (choose one of three):			
		1. upgrade to bRPC > 1.6.0, download link:			
		https://dist.apache.org/repos/dist/release/brpc/1.6.1/ 2. If you are using an old version of bRPC and hard to upgrade, you			
		can apply this patch: https://github.com/apache/brpc/pull/2411			
CVE-2023-45757	apache - brpc	3. disable rpcz feature	2023-10-16	6.1	Medium
		Reflected cross-site scripting (XSS) vulnerability on the Export for Translation page in Liferay Portal 7.4.3.4 through 7.4.3.85, and			
		Liferay DXP 7.4 before update 86 allows remote attackers to inject			
		arbitrary web script or HTML via the			
0.45.55.5	liferay - multiple	`_com_liferay_translation_web_internal_portlet_TranslationPortle		_	
CVE-2023-42497	products	t_redirect` parameter. Multiple reflected cross-site scripting (XSS) vulperabilities in the	2023-10-17	6.1	Medium
		Multiple reflected cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect			
		class in Liferay Portal 7.4.3.41 through 7.4.3.89, and Liferay DXP			
		7.4 update 41 through update 89 allow remote attackers to inject			
	liferay - multipla	arbitrary web script or HTML via the (1) code, or (2) error parameter. This issue is caused by an incomplete fix in CVE-2023-			
CVE-2023-44311	liferay - multiple products	33941.	2023-10-17	6.1	Medium
		Vulnerability in the Oracle Commerce Guided Search product of			
		Oracle Commerce (component: Workbench). The supported			
	oracle -	version that is affected is 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to			
		compromise Oracle Commerce Guided Search. Successful attacks			
1	commerce_guided_	compromise Oracle Commerce Guided Search. Successful attacks			

	T				1
		and while the vulnerability is in Oracle Commerce Guided Search,			
		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 Commerce Guided Search accessible data as well as unauthorized			
		read access to a subset of Oracle Commerce Guided Search			
		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).			
		Vulnerability in the Oracle Applications Framework product of			
		Oracle E-Business Suite (component: Personalization). 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 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			
		Applications Framework accessible data. CVSS 3.1 Base Score 6.1			
	oracle - e-	(Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22076	business_suite	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	6.1	Medium
		Vulnerability in the PeopleSoft Enterprise PeopleTools product of	_		
		Oracle PeopleSoft (component: PIA Core Technology). 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 require human interaction from a person other			
		than the attacker and while the vulnerability is in PeopleSoft			
		Enterprise PeopleTools, 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 PeopleSoft Enterprise PeopleTools accessible data as well as			
		unauthorized read access to a subset of PeopleSoft Enterprise			
	oracla militiral	PeopleTools accessible data. CVSS 3.1 Base Score 6.1			
CVE-2023-22080	oracle - multiple products	(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).	2023-10-17	6.1	Medium
CVL 2023-22000	products	Vulnerability in the Oracle Enterprise Command Center	2023 10-17	0.1	IVICUIUIII
		Framework product of Oracle E-Business Suite (component: UI			
		Components). Supported versions that are affected are ECC: 8, 9			
		and 10. Easily exploitable vulnerability allows unauthenticated			
		attacker with network access via HTTP to compromise Oracle			
		Enterprise Command Center Framework. Successful attacks			
		require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Command			
		Center 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 Enterprise Command Center Framework accessible data			
		as well as unauthorized read access to a subset of Oracle			
		Enterprise Command Center Framework accessible data. CVSS 3.1			
0) (5, 0000, 000)	oracle - multiple	Base Score 6.1 (Confidentiality and Integrity impacts). CVSS	2022		
CVE-2023-22107	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	6.1	Medium
		VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds			
		read vulnerability that exists in the functionality for sharing host			
		Bluetooth devices with the virtual machine. A malicious actor with			
		local administrative privileges on a virtual			
	vmware -	machine may be able to read privileged information contained in			
CVE-2023-34044	workstation	hypervisor memory from a virtual machine.	2023-10-20	6	Medium
		IDNA Converte Month Datable Co. D			
		IBM Security Verify Privilege On-Premises 11.5 could allow a			
		remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An			
	ibm -	attacker could exploit this vulnerability to obtain sensitive			
	security_verify_priv	information using man in the middle techniques. IBM X-Force ID:			
CVE-2022-22386	ilege_on-premises	221963.	2023-10-17	5.9	Medium
	<u> </u>	Vulnerability in the PL/SQL component of Oracle Database Server.			
		Supported versions that are affected are 19.3-19.20 and 21.3-			
		21.11. Easily exploitable vulnerability allows high privileged			
		attacker having Create Session, Execute on sys.utl_http privilege			
		with network access via Oracle Net to compromise PL/SQL.			
		Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PL/SQL, attacks			
		may significantly impact additional products (scope change).			
		Successful attacks of this vulnerability can result in unauthorized			
	oracle - multiple	update, insert or delete access to some of PL/SQL accessible data			
CVE-2023-22071	products	as well as unauthorized read access to a subset of PL/SQL	2023-10-17	5.9	Medium

	T	accessible data and unauthorized ability to sauce a partial denial of			1
		accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PL/SQL. CVSS 3.1 Base Score 5.9			
		(Confidentiality, Integrity and Availability impacts). CVSS Vector:			
		(CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L). Vulnerability in the Oracle FLEXCUBE Universal Banking product of			
		Oracle Financial Services Applications (component: Infrastructure).			
		Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and			
		14.5-14.7. Difficult to exploit vulnerability allows low privileged			
		attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human			
		interaction from a person other than the attacker. Successful			
		attacks of this vulnerability can result in unauthorized access to			
		critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or			
		delete access to some of Oracle FLEXCUBE Universal Banking			
		accessible data and unauthorized ability to cause a partial denial of			
		service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS			
	oracle - multiple	3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector:			
CVE-2023-22119	products	(CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L).	2023-10-17	5.9	Medium
		Vulnerability in the Oracle Banking Trade Finance product of			
		Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Difficult to			
		exploit vulnerability allows low privileged attacker with network			
		access via HTTP to compromise Oracle Banking Trade Finance.			
		Successful attacks require human interaction from a person other			
		than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all			
		Oracle Banking Trade Finance accessible data as well as			
		unauthorized update, insert or delete access to some of Oracle			
		Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking			
	oracle -	Trade Finance. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity			
	banking_trade_fina	and Availability impacts). CVSS Vector:			
CVE-2023-22122	nce	(CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L). Vulnerability in the Sun ZFS Storage Appliance product of Oracle	2023-10-17	5.9	Medium
		Systems (component: Core). The supported version that is			
		affected is 8.8.60. Difficult to exploit vulnerability allows			
		unauthenticated attacker with network access via HTTP to			
		compromise Sun ZFS Storage Appliance. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or			
	oracle -	frequently repeatable crash (complete DOS) of Sun ZFS Storage			
	sun_zfs_storage_ap	Appliance. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS			
CVE-2023-22130	pliance_kit	Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle Solaris product of Oracle Systems	2023-10-17	5.9	Medium
		(component: Kernel). 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 unauthorized ability to cause a hang or frequently			
		repeatable crash (complete DOS) of Oracle Solaris. Note: This			
		vunlerability only affects SPARC Systems. CVSS 3.1 Base Score 5.5			
CVE-2023-22129	oracle - solaris	(Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	5.5	Medium
	2.43.6 3014113	Stored cross-site scripting (XSS) vulnerability in the manage	_0_0 10 1/	3.5	caiaiii
		vocabulary page in Liferay Portal 7.4.2 through 7.4.3.87, and			
	liferay - multiple	Liferay DXP 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a			
CVE-2023-42629	products	Vocabulary's 'description' text field.	2023-10-17	5.4	Medium
	·	Multiple stored cross-site scripting (XSS) vulnerabilities in the			
		fragment components in Liferay Portal 7.4.2 through 7.4.3.53, and			
	liferay - multiple	Liferay DXP 7.4 before update 54 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into			
CVE-2023-44309	products	any non-HTML field of a linked source asset.	2023-10-17	5.4	Medium
		Stored cross-site scripting (XSS) vulnerability in Page Tree menu			
		Liferay Portal 7.3.6 through 7.4.3.78, and Liferay DXP 7.3 fix pack 1 through update 23, and 7.4 before update 79 allows remote			
	liferay - multiple	attackers to inject arbitrary web script or HTML via a crafted			
CVE-2023-44310	products	payload injected into page's "Name" text field.	2023-10-17	5.4	Medium
		Stored cross-site scripting (XSS) vulnerability in the Wiki widget in			
		Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and			
		earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows			
		remote attackers to inject arbitrary web script or HTML into a			
CVE_2022_42629	liferay - multiple	parent wiki page via a crafted payload injected into a wiki page's	2022 10 17	E 1	Madium
CVE-2023-42628	products	'Content' text field. Multiple stored cross-site scripting (XSS) vulnerabilities in the	2023-10-17	5.4	Medium
				i	1
		Commerce module in Liferay Portal 7.3.5 through 7.4.3.91, and			
CVE-2023-42627	liferay - multiple products	· · · · · · · · · · · · · · · · · · ·	2023-10-17	5.4	Medium

	T				
		crafted payload injected into a (1) Shipping Name, (2) Shipping			
		Phone Number, (3) Shipping Address, (4) Shipping Address 2, (5)			
		Shipping Address 3, (6) Shipping Zip, (7) Shipping City, (8) Shipping			
		Region (9), Shipping Country, (10) Billing Name, (11) Billing Phone			
		Number, (12) Billing Address, (13) Billing Address 2, (14) Billing Address 3, (15) Billing Zin, (16) Billing City, (17) Billing Region, (18)			
		Address 3, (15) Billing Zip, (16) Billing City, (17) Billing Region, (18) Billing Country, or (19) Region Code.			
		Vulnerability in the Oracle Business Intelligence Enterprise Edition			
		product of Oracle Analytics (component: Pod Admin). 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 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			
	oracle - multiple	5.4 (Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22082	products	(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	5.4	Medium
		Vulnerability in the BI Publisher product of Oracle Analytics			
		(component: Web 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 BI Publisher. Successful attacks require human			
		interaction from a person other than the attacker and while the			
		vulnerability is in BI Publisher, 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 BI Publisher accessible data as well as			
		unauthorized read access to a subset of BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity			
	oracle - multiple	impacts). CVSS Vector:			
CVE-2023-22105	products	(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	5.4	Medium
211 7072 77103	products	Vulnerability in the Oracle FLEXCUBE Universal Banking product of	2023 IU-I/	J. -1	MICUIUIII
		Oracle Financial Services Applications (component: Infrastructure).			
		Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and			
		14.5-14.7. Easily exploitable vulnerability allows low privileged			
		attacker with network access via HTTP to compromise Oracle			
		FLEXCUBE Universal Banking. Successful attacks require human			
		interaction from a person other than the attacker and while the			
		vulnerability is in Oracle FLEXCUBE Universal Banking, 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 FLEXCUBE Universal			
		Banking accessible data as well as unauthorized read access to a			
	_	subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS			
	oracle - multiple	3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS		_	
CVE-2023-22117	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	5.4	Medium
		Vulnerability in the Oracle Banking Trade Finance product of			
		Oracle Financial Services Applications (component: Infrastructure).			
		Supported versions that are affected are 14.5-14.7. Easily			
		exploitable vulnerability allows unauthenticated attacker with			
		network access via HTTP to compromise Oracle Banking Trade			
		Finance. 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 Banking Trade Finance accessible data as			
		well as unauthorized read access to a subset of Oracle Banking			
	oracle -	Trade Finance accessible data. CVSS 3.1 Base Score 5.4			
	banking_trade_fina	(Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22121	nce	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2023-10-17	5.4	Medium
		Vulnerability in the Oracle Banking Trade Finance product of		· · · · · ·	
		Oracle Financial Services Applications (component: Infrastructure).			
		Supported versions that are affected are 14.5-14.7. Easily			
		exploitable vulnerability allows low privileged attacker with			
		network access via HTTP to compromise Oracle Banking Trade			
		Finance. Successful attacks require human interaction from a			
		person other than the attacker and while the vulnerability is in			
		Oracle Banking Trade Finance, 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 Banking Trade Finance accessible data as			
	oracle	well as unauthorized read access to a subset of Oracle Banking			
	oracle -	Trade Finance accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22123	banking_trade_fina	(CONTIGENTIALITY and Integrity Impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	5.4	Medium
C 1 L-2 U 2 3-2 2 1 2 3	nce	\Cv33.3.1/\pay.iv/\pac.L/FN.L/OI.N/3.C/C.L/I.L/\pac.Iv).	ZUZ3-1U-1/	٥.4	ivicululli

CVE-2023-22124	oracle - banking_trade_fina nce	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, 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 Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance 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).	2023-10-17	5.4	Medium
CVE-2023-22125	oracle - banking_trade_fina nce	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, 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 Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance 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).	2023-10-17	5.4	Medium
CVE-2023-5561	wordpress - multiple products	The Popup Builder WordPress plugin through 4.1.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2023-10-16	5.3	Medium
CVE-2022-22377	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 221827.	2023-10-17	5.3	Medium
CVE-2021-38859	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a user to obtain version number information using a specially crafted HTTP request that could be used in further attacks against the system. IBM X-Force ID: 207899.	2023-10-17	5.3	Medium
CVE-2022-43889	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could disclose sensitive information through an HTTP request that could aid an attacker in further attacks against the system. IBM X-Force ID: 240452.	2023-10-17	5.3	Medium
CVE-2022-43891	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 240454.	2023-10-17	5.3	Medium
CVE-2022-43892	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 does not validate, or incorrectly validates, a certificate which could disclose sensitive information which could aid further attacks against the system. IBM X-Force ID: 240455.	2023-10-17	5.3	Medium
	oracle - multiple	Vulnerability in Oracle Java SE (component: CORBA). Supported versions that are affected are Oracle Java SE: 8u381 and 8u381-perf. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector:			
CVE-2023-22067 CVE-2023-22081	products oracle - multiple products	(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8 and 21. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK.	2023-10-17	5.3	Medium Medium

	T				
		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 for JDK. 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 5.3 (Availability impacts). CVSS Vector:			
		(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).			
		Vulnerability in the Oracle WebCenter Content product of Oracle			
		Fusion Middleware (component: Content Server). The supported			
		version that is affected is 12.2.1.4.0. Easily exploitable vulnerability			
		allows unauthenticated attacker with network access via HTTP to			
		compromise Oracle WebCenter Content. Successful attacks of this			
		vulnerability can result in unauthorized read access to a subset of			
		Oracle WebCenter Content accessible data. CVSS 3.1 Base Score			
	oracle -	5.3 (Confidentiality impacts). CVSS Vector:			
CVE-2023-22126	webcenter_content	(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-10-17	5.3	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). Supported versions that are			
		affected are 5.7.42 and prior and 8.0.31 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			
	amasla ii lii l	crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9			
CVE 2022 22045	oracle - multiple	(Availability impacts). CVSS Vector:	2022 40 47	4.0	N104:
CVE-2023-22015	products	(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	2023-10-17	4.9	Medium
		(component: Server: Optimizer). Supported versions that are			
		affected are 5.7.42 and prior and 8.0.31 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-2023-22026	products	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). Supported versions that are			
		affected are 5.7.43 and prior and 8.0.31 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			
OVE 2022 2022	oracle - multiple	(Availability impacts). CVSS Vector:	2022 12 17	4.0	N A 11
CVE-2023-22028	products	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.34 and prior and 8.1.0. 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			
	oracle - multiple	MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS			
CVE-2023-22032	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
	p. 544665	Vulnerability in the MySQL Server product of Oracle MySQL		5	Garaiii
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.34 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-2023-22064	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	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.			
CVE 2022 2225		CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	2022 40 47	4.0	N A = -1*
CVE-2023-22065	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
	oracla modelata	Vulnerability in the MySQL Server product of Oracle MySQL			
CVE-2023-22066	oracle - multiple products	(component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows	2023-10-17	4.9	Medium
	i DEQUUELS	ı o.o.o+ anu prior anu o.t.o. Easiiv expioilable vuinerabiiilly dilows	ZUZ3-TU-T/	4.5	i ivicululli

		1			I
		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:			
		(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 (component: InnoDB). Supported versions that are affected are			
		8.0.34 and prior and 8.1.0. 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-2023-22068	oracle - multiple products	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).	2023-10-17	4.9	Medium
<u>CVL 2023 22000</u>	products	Vulnerability in the MySQL Server product of Oracle MySQL	2023 10 17	7.3	IVICAIAIII
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.34 and prior and 8.1.0. 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			
	oracle - multiple	MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS			
CVE-2023-22070	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the Oracle Database Recovery Manager			
		component of Oracle Database Server. Supported versions that			
		are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having DBA account			
		privilege with network access via Oracle Net to compromise Oracle			
		Database Recovery Manager. Successful attacks of this			
		vulnerability can result in unauthorized ability to cause a hang or			
	1 100 1	frequently repeatable crash (complete DOS) of Oracle Database			
CVE-2023-22077	oracle - multiple products	Recovery Manager. 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).	2023-10-17	4.9	Medium
CVE-2023-22077	products	Vulnerability in the MySQL Server product of Oracle MySQL	2023-10-17	4.5	ivieululli
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.34 and prior and 8.1.0. 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			
	oracle - multiple	MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS			
CVE-2023-22078	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
	·	Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: InnoDB). Supported versions that are affected are			
		5.7.43 and prior, 8.0.34 and prior and 8.1.0. 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			
	oracle - multiple	MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS			
CVE-2023-22084	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Optimizer). Supported versions that are affected are 8.0.34 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-2023-22092	oracle musal	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).	2023-10-17	4.9	Medium
<u>CVE-2U23-22U92</u>	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL	2023-10-1/	4.9	ivieululli
		(component: InnoDB). Supported versions that are affected are			
		8.0.34 and prior and 8.1.0. 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.			
	oracle - multiple	CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:			
CVE-2023-22097	products	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL		-	
		(component: Server: Optimizer). Supported versions that are			
		affected are 8.0.34 and prior and 8.1.0. 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			
	oracle - multiple	MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS			
CVE-2023-22103	products	Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
	F : 2 2 2 2 2 2 2	,			

		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: InnoDB). Supported versions that are affected are		1	
		8.0.32 and prior. Easily exploitable vulnerability allows high		I	
		privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability		ĺ	
		can result in unauthorized ability to cause a hang or frequently		1	
		repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base		I	
		Score 4.9 (Availability impacts). CVSS Vector:		1	
CVE-2023-22104	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL		I	
		(component: Server: Optimizer). Supported versions that are		I	
		affected are 8.0.33 and prior. Easily exploitable vulnerability allows		I	
		high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this		I	
		vulnerability can result in unauthorized ability to cause a hang or		I	
		frequently repeatable crash (complete DOS) of MySQL Server.		I	
		CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:		I	
CVE-2023-22110	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL		I	
		(component: Server: UDF). Supported versions that are affected		I	
		are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to		I	
		compromise MySQL Server. Successful attacks of this vulnerability		I	
		can result in unauthorized ability to cause a hang or frequently		I	
		repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base		I	
		Score 4.9 (Availability impacts). CVSS Vector:		Ì	
CVE-2023-22111	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL		 I	
		(component: Server: Optimizer). Supported versions that are		I	
		affected are 8.0.34 and prior. Easily exploitable vulnerability allows		I	
		high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this		I	
		vulnerability can result in unauthorized ability to cause a hang or		I	
		frequently repeatable crash (complete DOS) of MySQL Server.		I	
		CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:		I	
CVE-2023-22112	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL		I	
		(component: InnoDB). Supported versions that are affected are		I	
		8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols		I	
		to compromise MySQL Server. Successful attacks of this		I	
		vulnerability can result in unauthorized ability to cause a hang or		I	
		frequently repeatable crash (complete DOS) of MySQL Server.		I	
	oracle - multiple	CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:		1	
CVE-2023-22114	products	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
		Vulnerability in the MySQL Server product of Oracle MySQL		1	
		(component: Server: DML). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high		I	
		privileged attacker with network access via multiple protocols to		,	
		compromise MySQL Server. Successful attacks of this vulnerability			
		compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently			
		can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base			
		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-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK.	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of	2023-10-17	4.9	Medium
CVE-2023-22115		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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8	2023-10-17	4.9	Medium
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector:			
CVE-2023-22115 CVE-2023-22091		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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	2023-10-17	4.9	Medium
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0,			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low			
CVE-2023-22115 CVE-2023-22091	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. 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.			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. 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. Successful attacks of this vulnerability can result in unauthorized			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0 and 12.2.1.4.0. 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. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0 and 12.2.1.4.0. 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. 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			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0 and 12.2.1.4.0. 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. 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			
	oracle - multiple	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: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0 and 12.2.1.4.0. 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. 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			

CVE-2023-35013	ibm - security_verify_gov ernance	IBM Security Verify Governance 10.0, Identity Manager could allow a local privileged user to obtain sensitive information from source code. IBM X-Force ID: 257769.	2023-10-16	4.4	Medium
CVE-2023-38719	ibm - db2	IBM Db2 11.5 could allow a local user with special privileges to cause a denial of service during database deactivation on DPF. IBM X-Force ID: 261607.	2023-10-17	4.4	Medium
CVE-2022-43893	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a privileged user to cause by using a malicious payload. IBM X-Force ID: 240634.	2023-10-17	4.4	Medium
CVE-2022-22384	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow an attacker to modify messages returned from the server due to hazardous input validation. IBM X-Force ID: 221961.	2023-10-17	4.3	Medium
CVE-2021-20581	ibm - security_verify_priv ilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a user to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 199324.	2023-10-17	4.3	Medium
	ibm - security_verify_priv	IBM Security Verify Privilege On-Premises 11.5 could allow an attacker to spoof a trusted entity due to improperly validating			
CVE-2022-22380	ilege_on-premises	certificates. IBM X-Force ID: 221957. Vulnerability in the Oracle Notification Server component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Notification Server executes to compromise Oracle Notification Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Notification Server accessible data. CVSS 3.1 Base Score 4.3	2023-10-17	4.3	Medium
CVE-2023-22073	oracle - multiple products	(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). Vulnerability in the Oracle Enterprise Session Border Controller	2023-10-17	4.3	Medium
	oracle - enterprise session	product of Oracle Communications (component: Web UI). Supported versions that are affected are 9.0-9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Session Border Controller. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector:			
CVE-2023-22083	_border_controller	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N). Vulnerability in the Oracle Communications Order and Service Management product of Oracle Communications Applications (component: User Management). Supported versions that are affected are 7.4.0 and 7.4.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Order and Service Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Order and Service Management accessible data. CVSS 3.1 Base	2023-10-17	4.3	Medium
CVE-2023-22088	oracle - multiple products oracle - multiple	Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector:	2023-10-17	4.3	Mediun
CVE-2023-22096	products	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-10-17	4.3	Medium
		In spring AMQP versions 1.0.0 to 2.4.16 and 3.0.0 to 3.0.9 , allowed list patterns for deserializable class			
CVE-2023-34050	vmware - multiple products	names were added to Spring AMQP, allowing users to lock down deserialization of	2023-10-19	4.3	Mediun

		data in messages from untrusted sources; however by default,			
		when no allowed list was provided, all classes could be deserialized.			
		list was provided, all classes could be describilized.			
		Specifically, an application is			
		vulnerable if			
		* the			
		SimpleMessageConverter or SerializerMessageConverter is used			
		* the user			
		does not configure allowed list patterns			
		* untrusted			
		message originators gain permissions to write messages to the			
		RabbitMQ			
		broker to send malicious content			
		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: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK:			
		17.0.8 and 21. 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 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			
	oracle - multiple	for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS			
CVE-2023-22025	products	Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2023-10-17	3.7	Low
	•	Vulnerability in the Oracle Solaris product of Oracle Systems			
		(component: Filesystem). Supported versions that are affected are			
		10 and 11. Difficult to exploit vulnerability allows unauthenticated			
		attacker with network access via rquota to compromise Oracle			
		Solaris. Successful attacks require human interaction from a			
		person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of			
		Oracle Solaris accessible data. CVSS 3.1 Base Score 3.1			
	oracle - multiple	(Confidentiality impacts). CVSS Vector:			
CVE-2023-22128	products	(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	2023-10-17	3.1	Low
		Vulnerability in the MySQL Server product of Oracle MySQL			
		(component: Server: Security: Encryption). 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 read access			
		to a subset of MySQL Server accessible data. CVSS 3.1 Base Score			
		2.7 (Confidentiality impacts). CVSS Vector:			
CVE-2023-22113	oracle - mysql	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2023-10-17	2.7	Low
	<u> </u>	Vulnerability in the Oracle Database Sharding component of			
		Oracle Database Server. Supported versions that are affected are			
		19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows			
		high privileged attacker having Create Session, Select Any Dictionary privilege with petwork access via Oracle Net to			
		Dictionary privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require			
		human interaction from a person other than the attacker.			
		Successful attacks of this vulnerability can result in unauthorized			
		ability to cause a partial denial of service (partial DOS) of Oracle			
	oracle - multiple	Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts).			
CVE-2023-22074	products	CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L).	2023-10-17	2.4	Low

		Vulnerability in the Oracle Database Sharding component of				1
		Oracle Database Server. Supported versions that are affected are				
		19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows				
		high privileged attacker having Create Session, Create Any View,				
		Select Any Table privilege with network access via Oracle Net to				
		compromise Oracle Database Sharding. Successful attacks require				
		human interaction from a person other than the attacker.				
		Successful attacks of this vulnerability can result in unauthorized				
		ability to cause a partial denial of service (partial DOS) of Oracle				
	oracle - multiple	Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts).				
CVE-2023-22075	products	CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L).	2023-10-17	2.4	Low	

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

Where NCA provides the vulnerability information as published by NIST's of individual's responsibility to ensure the implementation of appropriate recommendations.