KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Oracle Critical Patch Update, Oct 2022

Tracker ID: TN1022 **Date:** 21/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Oracle has issued a quarterly Critical Patch Update advisory for October 2022. It is a cumulative upgrade for numerous security vulnerabilities. This Critical Patch Update includes 370 new security patches for multiple product categories that address vulnerabilities in Oracle code and third-party components.

These vulnerabilities have been identified by independent researchers who have reported these flaws and exploitation attempts. Also, multiple remote code execution flaws have been discovered. In prior instances, attackers were successful in penetrating the network as targeted consumers did not deploy available updates. Therefore, it is strongly advised to identify vulnerable services, stay on actively supported versions, and deploy security fixes as soon as feasible.

Analysis: Affected Products and Versions

CVE ID	CVSS Score	Severity	Product	Component	Supported Versions Affected
CVE-2021-23450	9.8	Critical	Oracle Communications Convergence	Framework (dojo)	3.0.3.0
CVE-2021-43527	9.8	Critical	Oracle Communications Messaging Server	Security (NSS)	8.1
CVE-2022-23632	9.8	Critical	Oracle Communications Order and Service Management	Security (Traefik)	7.4
CVE-2020-10683	9.8	Critical	Oracle Commerce Platform	Dynamo Application Framework (dom4j)	11.3.0-11.3.2
CVE-2022-31813	9.8	Critical	Oracle Secure Backup	Oracle Secure Backup (Apache HTTP Server)	Prior to 18.1.0.2.0
CVE-2020-35169	9.8	Critical	Oracle GoldenGate	Oracle GoldenGate Microservices (Dell BSAFE Micro Edition Suite)	19c
CVE-2021-3918	9.8	Critical	Oracle Communications Unified Assurance	REST API (json-schema)	Prior to 5.5.7.0.0, 6.0.0.0.0
CVE-2022-31813	9.8	Critical	Oracle Communications Unified Assurance	User Interface (Apache HTTP Server)	Prior to 5.5.7.0.0, 6.0.0.0.0
CVE-2022-2068	9.8	Critical	Oracle Communications Unified Assurance	User Interface (OpenSSL)	Prior to 5.5.7.0.0, 6.0.0.0.0

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Oracle Critical Patch Update, Oct 2022

Tracker ID: TN1022 **Date:** 21/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

CVE ID	CVSS Score	Severity	Product	Component	Supported Versions Affected
CVE-2022-22978	9.8	Critical	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Signaling (Spring Security)	22.2.0
CVE-2022-1292	9.8	Critical	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Installer (OpenSSL)	22.2.1
CVE-2022-23218	9.8	Critical	Oracle Communications Cloud Native Core Unified Data Repository	Signaling (glibc)	22.1.1
CVE-2022-31813	9.8	Critical	Oracle Communications Diameter Signaling Router	Platform (Apache HTTP Server)	8.6.0.0
CVE-2021-21708	9.8	Critical	Oracle Communications Diameter Signaling Router	Platform (PHP)	8.6.0.0
CVE-2022-31813	9.8	Critical	Oracle Communications Element Manager	FEServer (Apache HTTP Server)	9
CVE-2022-22978	9.8	Critical	Oracle Communications Element Manager	Authentication (Spring Security)	9
CVE-2022-22978	9.8	Critical	Oracle Communications Interactive Session Recorder	Platform (Spring Security)	6.4
CVE-2021-31805	9.8	Critical	Oracle Communications Policy Management	Configuration Management Platform (Apache Struts)	12.6.0.0.0
CVE-2021-21783	9.8	Critical	Oracle Communications User Data Repository	Platform (gSOAP)	12.4.0
CVE-2022-31813	9.8	Critical	Oracle Communications User Data Repository	Platform (Apache HTTP Server)	12.4.0
CVE-2021-43527	9.8	Critical	Oracle Communications User Data Repository	Platform (NSS)	12.4.0
CVE-2021-23450	9.8	Critical	Oracle Communications WebRTC Session Controller	Platform (dojo)	7.2.0, 7.2.1
CVE-2022-31813	9.8	Critical	Oracle Enterprise Operations Monitor	User Login (Apache HTTP Server)	4.4, 5.0

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Oracle Critical Patch Update, Oct 2022

Tracker ID: TN1022 **Date:** 21/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

CVE ID	CVSS Score	Severity	Product	Component	Supported Versions Affected
CVE-2021-44790	9.8	Critical	Oracle SD-WAN Edge	Management (Apache HTTP Server)	7.0.7
CVE-2022-22978	9.8	Critical	Oracle SD-WAN Edge	Management (Spring Security)	9.1.1.2.0
CVE-2022-23305	9.8	Critical	Application Management Pack for Oracle E-Business Suite	EBS EM Plugin (Apache Log4j)	13.4.1.0.0
CVE-2022-21587	9.8	Critical	Oracle Web Applications Desktop Integrator	Upload	12.2.3-12.2.11
CVE-2022-39428	9.8	Critical	Oracle Web Applications Desktop Integrator	Upload	12.2.3-12.2.11
CVE-2018-1285	9.8	Critical	Enterprise Manager Base Platform	Application Service Level Management (Apache log4net)	13.4.0.0
CVE-2021-23450	9.8	Critical	Enterprise Manager Ops Center	Networking (dojo)	12.4.0.0
CVE-2022-23457	9.8	Critical	Oracle Financial Services Analytical Applications Infrastructure	Others (Enterprise Security API)	8.0.7.0-8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1
CVE-2022-33980	9.8	Critical	Oracle Business Intelligence Enterprise Edition	BI Application Archive (Apache Commons Configuration)	5.9.0.0, 6.4.0.0
CVE-2019-17195	9.8	Critical	Oracle Data Integrator	WLS Configuration Template (Nimbus JOSE+JWT)	12.2.1.4.0
CVE-2022-23943	9.8	Critical	Oracle HTTP Server	SSL Module (Apache HTTP Server)	12.2.1.3.0, 12.2.1.4.0
CVE-2022-23305	9.8	Critical	Oracle Middleware Common Libraries and Tools	Third Party Patch (Apache Log4j)	12.2.1.3.0
CVE-2022-25315	9.8	Critical	Oracle Outside In Technology	Outside In Filters (LibExpat)	8.5.6
CVE-2022-23305	9.8	Critical	Oracle WebCenter Content	Web Content Management (Apache Log4j)	12.2.1.3.0

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Oracle Critical Patch Update, Oct 2022

Tracker ID: TN1022 **Date:** 21/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

CVE ID	CVSS Score	Severity	Product	Component	Supported Versions Affected
CVE-2021-23450	9.8	Critical	Oracle WebCenter Portal	Security Framework (dojo)	12.2.1.3.0, 12.2.1.4.0
CVE-2021-23450	9.8	Critical	Oracle WebCenter Sites	Centralized Thirdparty Jars (dojo)	12.2.1.3.0, 12.2.1.4.0
CVE-2022-32532	9.8	Critical	Oracle WebCenter Sites	WebCenter Sites (Apache Shiro)	12.2.1.3.0, 12.2.1.4.0
CVE-2022-33980	9.8	Critical	Oracle Hyperion Infrastructure Technology	Installation and Configuration (Apache Commons Configuration)	11.2.9
CVE-2021-43527	9.8	Critical	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure SEC (NSS)	9.2.6.3 and prior
CVE-2022-1292	9.8	Critical	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure SEC (OpenSSL)	9.2.6.3 and prior
CVE-2022-32207	9.8	Critical	MySQL Enterprise Backup	Enterprise Backup: Security (cURL)	4.1.4 and prior
CVE-2022-23305	9.8	Critical	Oracle Agile Engineering Data Management	Installation Issues (Apache Log4j)	6.2.1.0
CVE-2022-22978	9.8	Critical	Oracle Utilities Testing Accelerator	Tools (Spring Security)	6.0.0.1.3, 6.0.0.2.4, 6.0.0.3.3
CVE-2022-1586	9.1	Critical	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Signaling (PCRE2)	22.2.1
CVE-2022-1586	9.1	Critical	Oracle Communications Cloud Native Core Unified Data Repository	Signaling (PCRE2)	22.3.0
CVE-2019-3862	9.1	Critical	Oracle Communications User Data Repository	Platform (libssh2)	12.4.0
CVE-2022-32215	9.1	Critical	Oracle GraalVM Enterprise Edition	Node (Node.js)	Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3, 22.2.0

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Oracle Critical Patch Update, Oct 2022

Tracker ID: TN1022 **Date:** 21/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible. Refer to the complete list of affected products here.
- Monitor the services and critical assets exposed to the Internet. Collect and review relevant logs, data, and artifacts to identify any threat in the network.

References

- Oracle, Oracle Critical Patch Update Advisory - October 2022, 18th October 2022, External Link (www.oracle.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471