CVE-2023-2650

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-2650
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-30 14:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impa

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link	Tags
www.openssl.org/news/secadv/20230530.txt	MISC	www.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
Debian -- Security Information -- DSA-5417-1 openssl	MISC	www.debian.org	
[SECURITY] [DLA 3449-1] openssl security update	MISC	lists.debian.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
403 Forbidden	MISC	security.netapp.com	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		security.gentoo.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com	
October 2023 MySQL Server Vulnerabilities in NetApp Products | NetApp Product Security	MISC	security.netapp.com	

Security Advisory	MISC	psirt.global.sonicwall.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160752 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-3722)

161096 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-6330)

181818 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5417-1)

181834 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3449-1)

183591 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-2650)

199379 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6119-1)

199503 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-6188-1)

200161 Ubuntu Security Notification for Node.js Vulnerabilities (USN-6672-1)

20369 Oracle MySQL OCT 2023 Critical Patch Update (CPUOCT2023)

241736 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:3722)

242308 Red Hat Update for edk2 security (RHSA-2023:6330)

242553 Red Hat Update for JBoss Core Services (RHSA-2023:7625)

330149 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory39)

355387 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2023-2073

355428 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2023-1762

355470 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-222

355523 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2023-422

355550 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL)11 : ALAS2-2023-2097

356233 Amazon Linux Security Advisory for openssl-snapsafe : ALASOPENSSL-SNAPSAFE-2023-002

356483 Amazon Linux Security Advisory for openssl-snapsafe : ALAS2OPENSSL-SNAPSAFE-2023-002

357333 Amazon Linux Security Advisory for edk2 : ALAS2-2024-2502

378948 Oracle Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (CPUOCT2023)

379141 SolarWinds Serv-U HTML Injection Vulnerability

503023 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503024 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

503025 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503121 Alpine Linux Security Update for openssl

505906 Alpine Linux Security Update for openssl

673266 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2593)

673271 EulerOS Security Update for shim (EulerOS-SA-2023-2598)

673297 EulerOS Security Update for shim (EulerOS-SA-2023-2628)

673308 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2623)

673357 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2835)

673365 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3141)

673366 EulerOS Security Update for shim (EulerOS-SA-2023-2801)

673398 EulerOS Security Update for linux-sgx (EulerOS-SA-2023-3047)

673410 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2830)

673487 EulerOS Security Update for shim (EulerOS-SA-2023-2831)

673596 EulerOS Security Update for compat-openssl10 (EulerOS-SA-2023-3117)

673724 EulerOS Security Update for shim (EulerOS-SA-2024-1299)

674010 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2793)

674017 EulerOS Security Update for shim (EulerOS-SA-2023-2836)

674047 EulerOS Security Update for shim (EulerOS-SA-2023-2825)

674048 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2817)

691177 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (eb9a3c57-ff9e-11ed-a0d1-84a93843eb75)

691183 Free Berkeley Software Distribution (FreeBSD) Security Update for python (d86becfe-05a4-11ee-9d4a-080027eda32c)

691336 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (22df5074-71cd-11ee-85eb-84a93843eb75)

710857 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)

730953 Hewlett Packard Enterprise (HPE) OneView Multiple Vulnerabilities

754048 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_0_0 (OpenSSL1_0_0)(SUSE-SU-2023:2331-1)

754049 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_0_0 (OpenSSL-1_0_0) (SUSE-SU-2023:2330-1)

754050 SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:2329-1)

754051 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_1 (OpenSSL-1_1) (SUSE-SU-2023:2328-1)

754052 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_1 (OpenSSL-1_1) (SUSE-SU-2023:2327-1)

754064 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:2343-1)

906953 Common Base Linux Mariner (CBL-Mariner) Security Update for kata-containers-cc (27009-1)

907009 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (26979-1)

907024 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (26984-1)

907591 Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31144-1)

941150 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:3722)

941346 AlmaLinux Security Update for edk2 (ALSA-2023:6330)