CVE-2023-0464

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-0464
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-22 17:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certifica

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link	Tags
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	
Enterprise Security Alerts & Advisories for Couchbase		www.couchbase.com	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		security.gentoo.org	
www.openssl.org/news/secadv/20230322.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	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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)

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)

183828 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0464)

199305 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6039-1)

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

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)

355097 Amazon Linux Security Advisory for openssl11 : ALAS2-2023-2039

355167 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-181

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

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

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

378679 Oracle Managed Virtualization (VM) VirtualBox Linux Multiple Vulnerabilities (CPUJUL2023)

378680 Oracle Managed Virtualization (VM) VirtualBox Windows Multiple Vulnerabilities (CPUJUL2023)

379141 SolarWinds Serv-U HTML Injection Vulnerability

379220 GitLab Multiple Security Vulnerabilities (gitlab- 15.11.1, 15.10.5, and 15.9.6)

379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)

38893 OpenSSL Invalid certificate policies

502681 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

502682 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

502683 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL) 3

502758 Alpine Linux Security Update for openssl

502908 Alpine Linux Security Update for openssl1.1-compat

503022 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503118 Alpine Linux Security Update for openssl

505785 Alpine Linux Security Update for openssl1.1-compat

505903 Alpine Linux Security Update for openssl

672905 EulerOS Security Update for shim (EulerOS-SA-2023-1830)

672930 EulerOS Security Update for shim (EulerOS-SA-2023-1812)

672941 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1807)

672943 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1825)

672984 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1875)

673006 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1850)

673062 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2195)

673095 EulerOS Security Update for compat-openssl10 (EulerOS-SA-2023-2187)

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

673566 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2702)

673605 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2660)

673941 EulerOS Security Update for shim (EulerOS-SA-2023-2909)

674034 EulerOS Security Update for shim (EulerOS-SA-2023-2890)

691099 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (1ba034fb-ca38-11ed-b242-d4c9ef517024)

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

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

753863 SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:1737-1)

753879 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:1704-1)

753880 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:1703-1)

753884 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1748-1)

753885 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1747-1)

753896 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1790-1)

906793 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (25697-1)

906803 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (25709-1)

906945 Common Base Linux Mariner (CBL-Mariner) Security Update for kata-containers-cc (26731-1)

907371 Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31141-1)

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