CVE-2023-0465

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-0465
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-28 15:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to

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
www.openssl.org/news/secadv/20230328.txt	MISC	www.openssl.org	
Debian -- Security Information -- DSA-5417-1 openssl	MISC	www.debian.org	
[SECURITY] [DLA 3449-1] openssl security update	MISC	lists.debian.org	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		security.gentoo.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
March 2023 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security	MISC	security.netapp.com	
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)

183838 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0465)

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

379141 SolarWinds Serv-U HTML Injection Vulnerability

38893 OpenSSL Invalid certificate policies

502694 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

502695 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

502696 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

502759 Alpine Linux Security Update for openssl

502909 Alpine Linux Security Update for openssl1.1-compat

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

503119 Alpine Linux Security Update for openssl

505786 Alpine Linux Security Update for openssl1.1-compat

505904 Alpine Linux Security Update for openssl

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)

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)

673173 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2317)

673178 EulerOS Security Update for shim (EulerOS-SA-2023-2324)

673200 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2337)

673205 EulerOS Security Update for shim (EulerOS-SA-2023-2344)

673231 EulerOS Security Update for shim (EulerOS-SA-2023-2369)

673243 EulerOS Security Update for shim (EulerOS-SA-2023-2395)

673331 EulerOS Security Update for shim (EulerOS-SA-2023-2711)

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)

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

674033 EulerOS Security Update for shim (EulerOS-SA-2023-2669)

691102 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (425b9538-ce5f-11ed-ade3-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)

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

753898 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1794-1)

753923 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1908-1)

753924 SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:1912-1)

753927 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:1922-1)

754004 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:1914-1)

906787 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (25951-1)

906849 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (25937-1)

907019 Common Base Linux Mariner (CBL-Mariner) Security Update for kata-containers-cc (27241-1)

907543 Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31145-1)

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