CVE-2023-5678

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-5678
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-06 16:15:00 UTC
Updated	2023-11-30 22:15:00 UTC
Description	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters m

Risk And Classification

Problem Types: CWE-754

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	
security.netapp.com/advisory/ntap-20231130-0010		security.netapp.com	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
/err404.html	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	
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com	
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

161251 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-7877)

161287 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2024-12056)

200094 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6622-1)

200107 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6632-1)

200215 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6709-1)

242632 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:7877)

242687 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2024:0154)

242696 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2024:0208)

243077 Red Hat Update for JBoss Core Services (RHSA-2024:1316)

330164 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory40)

356767 Amazon Linux Security Advisory for openssl11 : ALAS2-2023-2351

356770 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2023-2350

356780 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2023-1891

356891 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL)-snapsafe : ALAS2OPENSSL-SNAPSAFE-2023-004

356903 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-443

356993 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2023-477

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

379545 Splunk Enterprise Third Party Package Updates for March 2024 (SVD-2024-0303)

379546 Splunk Universal Forwarder Third Party Package Updates for March 2024 (SVD-2024-0304)

379630 Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2024:0047)

503552 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503621 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503687 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

504259 Alpine Linux Security Update for openssl

505911 Alpine Linux Security Update for openssl

673338 EulerOS Security Update for shim (EulerOS-SA-2024-1098)

673343 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1125)

673443 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1069)

673480 EulerOS Security Update for shim (EulerOS-SA-2024-1129)

673598 EulerOS Security Update for compat-openssl10 (EulerOS-SA-2024-1258)

673684 EulerOS Security Update for shim (EulerOS-SA-2024-1164)

673687 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1184)

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

673737 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1287)

673773 EulerOS Security Update for linux-sgx (EulerOS-SA-2024-1124)

673790 EulerOS Security Update for shim (EulerOS-SA-2024-1186)

673797 EulerOS Security Update for shim-signed (EulerOS-SA-2024-1165)

673858 EulerOS Security Update for openssl111d (EulerOS-SA-2024-1157)

673889 EulerOS Security Update for shim (EulerOS-SA-2024-1113)

673908 EulerOS Security Update for shim (EulerOS-SA-2024-1206)

673915 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1155)

673962 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1204)

674007 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1093)

674055 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1109)

674097 EulerOS Security Update for shim (EulerOS-SA-2024-1074)

691351 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (a5956603-7e4f-11ee-9df6-84a93843eb75)

755307 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4524-1)

755308 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:4523-1)

755309 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:4522-1)

755310 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4521-1)

755311 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4520-1)

755312 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4519-1)

755313 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4518-1)

755361 SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:4593-1)

755375 SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:4635-1)

755461 SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:4649-1)

755503 SUSE Enterprise Linux Security Update for openssl-1_1-livepatches (SUSE-SU-2023:4919-1)

755504 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1-livepatches (SUSE-SU-2023:4918-1)

907698 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (31880-1)

907730 Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31872-1)

941507 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:7877)