CVE-2023-3446

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-3446
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-19 12:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that u

Risk And Classification

Problem Types: CWE-1333

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.2	-	All	All
Application	Openssl	Openssl	1.1.1	-	All	All
Application	Openssl	Openssl	3.0.0	-	All	All
Application	Openssl	Openssl	3.1.0	-	All	All
Application	Openssl	Openssl	3.1.1	-	All	All

References

Reference	Source	Link	Tags
www.openssl.org/news/secadv/20230719.txt	MISC	www.openssl.org	
[SECURITY] [DLA 3530-1] openssl security update	MISC	lists.debian.org	
oss-security - OpenSSL Security Advisory	MISC	www.openwall.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 - Re: OpenSSL Security Advisory	MISC	www.openwall.com	
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com	
CVE-2023-3446 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	

oss-security - Re: OpenSSL Security Advisory	MISC	www.openwall.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, analys

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)
- 161366 Oracle Enterprise Linux Security Update for edk2 (ELSA-2024-0888)
- 199838 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6435-1)
- 199860 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6450-1)
- 199865 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6435-2)
- 200215 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6709-1)
- 242553 Red Hat Update for JBoss Core Services (RHSA-2023:7625)
- 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)
- 242858 Red Hat Update for edk2 (RHSA-2024:0408)
- 242981 Red Hat Update for edk2 (RHSA-2024:0888)
- 243098 Red Hat Update for edk2 (RHSA-2024:1415)
- 296105 Oracle Solaris 11.4 Support Repository Update (SRU) 63.157.1 Missing (CPUOCT2023)
- 330149 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory39)
- 355881 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-306
- 356346 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2023-449
- 356356 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2023-1843
- 356509 Amazon Linux Security Advisory for openssl-snapsafe : ALAS2OPENSSL-SNAPSAFE-2023-003
- 357333 Amazon Linux Security Advisory for edk2 : ALAS2-2024-2502

379050 Splunk Enterprise Multiple Vulnerabilities (SVD-2023-1104,SVD-2023-1105)

379095 Splunk Universal Forwarder Multiple Vulnerabilities (SVD-2023-1107)

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

503045 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503046 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)3

503053 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503054 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)1.1-compat

503123 Alpine Linux Security Update for openssl

505787 Alpine Linux Security Update for openssl1.1-compat

505908 Alpine Linux Security Update for openssl

6000160 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3530-1)

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

673405 EulerOS Security Update for openssl098e (EulerOS-SA-2024-1156)

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

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

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

673771 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2847)

673782 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2864)

673804 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2902)

673807 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2883)

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

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

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

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

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

674045 EulerOS Security Update for shim (EulerOS-SA-2023-3044)

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

674049 EulerOS Security Update for shim (EulerOS-SA-2023-3021)

674091 EulerOS Security Update for shim (EulerOS-SA-2023-3232)

674115 EulerOS Security Update for shim (EulerOS-SA-2023-3197)

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

754207 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1 (SUSE-SU-2023:2961-1)

754213 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1 (SUSE-SU-2023:2964-1)

754220 SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:3012-1)

754229 SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:3096-1)

754231 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_0_0 (SUSE-SU-2023:3093-1)

754245 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1 (SUSE-SU-2023:3179-1)

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

941587 AlmaLinux Security Update for edk2 (ALSA-2024:0888)