CVE-2023-3817

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-3817
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-31 16:15:00 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-834

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0.2	-	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.2g	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All
Application	Openssl	Openssl	1.0.2j	All	All	All
Application	Openssl	Openssl	1.0.2k	All	All	All
Application	Openssl	Openssl	1.0.2l	All	All	All

Application	Openssl	Openssl	1.0.2m	All	All	All
Application	Openssl	Openssl	1.0.2n	All	All	All
Application	Openssl	Openssl	1.0.2o	All	All	All
Application	Openssl	Openssl	1.0.2p	All	All	All
Application	Openssl	Openssl	1.0.2q	All	All	All
Application	Openssl	Openssl	1.0.2r	All	All	All
Application	Openssl	Openssl	1.0.2s	All	All	All
Application	Openssl	Openssl	1.0.2t	All	All	All
Application	Openssl	Openssl	1.0.2u	All	All	All
Application	Openssl	Openssl	1.0.2v	All	All	All
Application	Openssl	Openssl	1.0.2w	All	All	All
Application	Openssl	Openssl	1.0.2x	All	All	All
Application	Openssl	Openssl	1.0.2y	All	All	All
Application	Openssl	Openssl	1.0.2za	All	All	All
Application	Openssl	Openssl	1.0.2zb	All	All	All
Application	Openssl	Openssl	1.0.2zc	All	All	All
Application	Openssl	Openssl	1.0.2zd	All	All	All
Application	Openssl	Openssl	1.0.2ze	All	All	All
Application	Openssl	Openssl	1.0.2zf	All	All	All
Application	Openssl	Openssl	1.0.2zg	All	All	All
Application	Openssl	Openssl	1.0.2zh	All	All	All
Application	Openssl	Openssl	1.1.1	-	All	All
Application	Openssl	Openssl	1.1.1	pre1	All	All
Application	Openssl	Openssl	1.1.1	pre2	All	All
Application	Openssl	Openssl	1.1.1	pre3	All	All
Application	Openssl	Openssl	1.1.1	pre4	All	All
Application	Openssl	Openssl	1.1.1	pre5	All	All
Application	Openssl	Openssl	1.1.1	pre6	All	All
Application	Openssl	Openssl	1.1.1	pre7	All	All
Application	Openssl	Openssl	1.1.1	pre8	All	All
Application	Openssl	Openssl	1.1.1	pre9	All	All
Application	Openssl	Openssl	1.1.1a	All	All	All
Application	Openssl	Openssl	1.1.1b	All	All	All
Application	Openssl	Openssl	1.1.1c	All	All	All
Application	Openssl	Openssl	1.1.1d	All	All	All

Application	Openssl	Openssl	1.1.1e	All	All	All
Application	Openssl	Openssl	1.1.1f	All	All	All
Application	Openssl	Openssl	1.1.1g	All	All	All
Application	Openssl	Openssl	1.1.1h	All	All	All
Application	Openssl	Openssl	1.1.1i	All	All	All
Application	Openssl	Openssl	1.1.1j	All	All	All
Application	Openssl	Openssl	1.1.1k	All	All	All
Application	Openssl	Openssl	1.1.1l	All	All	All
Application	Openssl	Openssl	1.1.1m	All	All	All
Application	Openssl	Openssl	1.1.1n	All	All	All
Application	Openssl	Openssl	1.1.1o	All	All	All
Application	Openssl	Openssl	1.1.1p	All	All	All
Application	Openssl	Openssl	1.1.1q	All	All	All
Application	Openssl	Openssl	1.1.1r	All	All	All
Application	Openssl	Openssl	1.1.1s	All	All	All
Application	Openssl	Openssl	1.1.1t	All	All	All
Application	Openssl	Openssl	1.1.1u	All	All	All

References

Reference	Source	Link
CVE-2023-3817 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org
[SECURITY] [DLA 3530-1] 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
oss-security - Re: illumos (or at least danmcd) membership in the distros list	MISC	www.openwall.com
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com
www.openssl.org/news/secadv/20230731.txt	MISC	www.openssl.org
SecLists.Org Security Mailing List Archive	MISC	seclists.org
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org
CVE-2023-3817 MySQL Connector/ODBC Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com
oss-security - Re: illumos (or at least danmcd) membership in the distros list	MISC	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)

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)

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)

355853 Amazon Linux Security Advisory for edk2 : ALAS2-2023-2205

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)

379266 Oracle Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (CPUJAN2024)

379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)

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

503089 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503090 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503124 Alpine Linux Security Update for openssl

503323 Alpine Linux Security Update for openssl3

505909 Alpine Linux Security Update for openssl

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

673341 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3225)

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

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

673476 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3190)

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

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

673749 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3016)

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)

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

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

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

674089 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3039)

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

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

691222 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (bad6588e-2fe0-11ee-a0d1-84a93843eb75)

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)

754259 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1 (SUSE-SU-2023:3239-1)

754280 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_0_0 (SUSE-SU-2023:3339-1)

755030 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:3958-1)

755035 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:3291-2)

755152 SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:4190-1)

755153 SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:4189-1)

907265 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (27817-1)

907561 Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31139-1)

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