CVE-2022-2097

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-2097
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-05 11:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Clustered Data Ontap Antivirus Connector	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Openssl	Openssl	All	All	All	All

Application	Siemens	Sinec Ins	All	All	All	All
Application	Siemens	Sinec Ins	1.0	-	All	All
Application	Siemens	Sinec Ins	1.0	sp1	All	All
Application	Siemens	Sinec Ins	1.0	sp2	All	All

References

Reference	Source	Link
CVE-2022-2097 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
CVE-2022-2097 MySQL Server Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 36 Update: openssl-3.0.5-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
OpenSSL: Multiple Vulnerabilities (GLSA 202210-02) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 36 Update: openssl1.1-1.1.1q-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org
[SECURITY] Fedora 35 Update: openssl-1.1.1q-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
[SECURITY] Fedora 36 Update: openssl-3.0.5-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Debian -- Security Information -- DSA-5343-1 openssl	DEBIAN	www.debian.org
[SECURITY] Fedora 35 Update: openssl-1.1.1q-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org
[SECURITY] Fedora 36 Update: openssl1.1-1.1.1q-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
cert-portal.siemens.com/productcert/pdf/ssa-332410.pdf	CONFIRM	cert-portal.siemens.com
www.openssl.org/news/secadv/20220705.txt	CONFIRM	www.openssl.org
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
[SECURITY] [DLA 3325-1] openssl security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Alex Chernyakhovsky

Legacy QID Mappings

160014 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-5818)

160025 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-9683)

160072 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-6234)

160072 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-6224)

181546 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5343-1)

181593 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3325-1)

184089 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-2097)

198850 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-5502-1)

199873 Ubuntu Security Notification for Node.js Vulnerabilities (USN-6457-1)

20273 Oracle MySQL October 2022 Critical Patch Update (CPUOCT2022)

240588 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2022:5818)

240641 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2022:6224)

282924 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-3fdc2d3047)

282939 Fedora Security Update for openssl1.1 (FEDORA-2022-89a17be281)

282968 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-41890e9e44)

296083 Oracle Solaris 11.4 Support Repository Update (SRU) 49.126.2 Missing (CPUOCT2022)

296084 Oracle Solaris 11.4 Support Repository Update (SRU) 50.126.3 Missing (CPUOCT2022)

296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)

330109 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Arbritary Code Execution Vulnerability (openssl_advisory36)

354286 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-147

354459 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-195

354579 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2022-195

354802 Amazon Linux Security Advisory for openssl11 : ALAS2-2023-1974

355250 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-051

355252 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-054

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

377563 Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2022:0148)

377645 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUOCT2022)

377651 Oracle MYSQL Connector/ODBC Critical Patch Update (CPU) October 2022 (CPUOCT2022)

379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)

502413 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

502416 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL 3)

502416 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

502753 Alpine Linux Security Update for openssl

502906 Alpine Linux Security Update for openssl1.1-compat

591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

672094 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2300)

672096 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2329)

672162 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2419)

672172 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2432)

672193 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2476)

672447 EulerOS Security Update for linux-sgx (EulerOS-SA-2022-2852)

673086 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL)111d (EulerOS-SA-2023-2162)

690892 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (a28e8b7e-fc70-11ec-856e-d4c9ef517024)

690894 Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (b9210706-feb0-11ec-81fa-1c697a616631)

690971 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (4b9c1c17-587c-11ed-856e-d4c9ef517024)

710638 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202210-02)

752298 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2022:2308-1)

752301 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2022:2309-1)

752305 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2022:2311-1)

752308 SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2022:2306-1)

752310 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2022:2312-1)

752325 SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2022:2328-1)

902455 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10126)

902472 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10113)

902554 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10109)

904808 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10122-1)

906025 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10122-2)

906368 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10109-2)

940611 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2022:5818)

940611 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2022:5818)

940649 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2022:6224)

960214 Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2022:5818)