CVE-2023-5363

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-5363
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2024-02-01 17:15:00 UTC
Description	Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths. This can lead to pot

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	12.0	All	All	All
Hardware	Netapp	H300s	All	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	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	All	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	All	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org
January 2024 MySQL Server 8.0.35 Vulnerabilities in NetApp Products | NetApp Product Security		security.netapp.com

www.openssl.org/news/secadv/20231024.txt	MISC	www.openssl.org
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com
CVE-2023-5363 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com
CVE-2023-5363 MySQL Connector/ODBC Vulnerability in NetApp Products | NetApp Product Security		security.netapp.com
Debian -- Security Information -- DSA-5532-1 openssl	MISC	www.debian.org
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

- 161307 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2024-0310)
- 161316 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2024-12093)
- 199860 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6450-1)
- 20398 Oracle MySQL JAN 2024 Critical Patch Update (CPUJAN2024)
- 242763 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2024:0500)
- 242865 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2024:0310)
- 296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
- 330164 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory40)
- 356621 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-406
- 503438 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
- 503439 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
- 505910 Alpine Linux Security Update for openssl
- 6000294 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5532-1)
- 691337 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (4a4712ae-7299-11ee-85eb-84a93843eb75)
- 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)
- 941548 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2024:0310)