CVE-2023-1255

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-1255
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-20 17:15:00 UTC
Updated	2023-09-08 17:15:00 UTC
Description	Issue summary: The AES-XTS cipher decryption implementation for 64 bit ARM platform contains a bug that could cause it

Risk And Classification

Problem Types: CWE-125

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	
CVE-2023-1255 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com	
/err404.html	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 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

160752 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-3722)

184876 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-1255)

199379 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6119-1)

241736 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:3722)

355167 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-181

379141 SolarWinds Serv-U HTML Injection Vulnerability

502981 Alpine Linux Security Update for openssl3

502989 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503120 Alpine Linux Security Update for openssl

505905 Alpine Linux Security Update for openssl

941150 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:3722)