CVE-2022-3358

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-3358
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-11 15:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated function ca

Risk And Classification

Problem Types: CWE-476

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		git.openssl.org	
Security Advisory	CONFIRM	psirt.global.sonicwall.com	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		security.gentoo.org	
CVE-2022-3358 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org	
www.openssl.org/news/secadv/20221011.txt	CONFIRM	www.openssl.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

LEGACY: Chris Rapier (Pittsburgh Supercomputing Center)

Legacy QID Mappings

160603 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-2523)

184216 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-3358)

199012 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

199113 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

199114 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

199115 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

199116 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

199117 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

241433 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:2523)

330128 IBM AIX Multiple Vulnerabilities in Open Secure Sockets Layer (OpenSSL) (openssl_advisory37)

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

502539 Alpine Linux Security Update for openssl3

502754 Alpine Linux Security Update for openssl

690962 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (7392e1e3-4eb9-11ed-856e-d4c9ef517024)

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

752752 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-3) (SUSE-SU-2022:3843-1)

941019 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:2523)