



# CVE-2022-3358

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-3358
<b>State</b>	PUBLIC
<b>Assigner</b>	openssl-security@openssl.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-10-11 15:15:00 UTC
<b>Updated</b>	2024-02-04 09:15:00 UTC
<b>Description</b>	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		<a href="https://git.openssl.org">git.openssl.org</a>	
Security Advisory	CONFIRM	<a href="https://psirt.global.sonicwall.com">psirt.global.sonicwall.com</a>	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		<a href="https://security.gentoo.org">security.gentoo.org</a>	
CVE-2022-3358 OpenSSL Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	<a href="https://git.openssl.org">git.openssl.org</a>	
<a href="https://www.openssl.org/news/secadv/20221011.txt">www.openssl.org/news/secadv/20221011.txt</a>	CONFIRM	<a href="https://www.openssl.org">www.openssl.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, :

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Chris Ravier (Pittsburgh Supercomputing Center)

## Legacy QID Mappings

<a href="#">160603</a> Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-2523)
<a href="#">184216</a> Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-3358)
<a href="#">199012</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)
<a href="#">199113</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)
<a href="#">199114</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)
<a href="#">199115</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)
<a href="#">199116</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)
<a href="#">199117</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)
<a href="#">241433</a> Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:2523)
<a href="#">330128</a> IBM AIX Multiple Vulnerabilities in Open Secure Sockets Layer (OpenSSL) (openssl_advisory37)
<a href="#">355252</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-054
<a href="#">502539</a> Alpine Linux Security Update for openssl3
<a href="#">502754</a> Alpine Linux Security Update for openssl
<a href="#">690962</a> Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (7392e1e3-4eb9-11ed-856e-d4c9ef517024)
<a href="#">710857</a> Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)
<a href="#">752752</a> SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-3) (SUSE-SU-2022:3843-1)
<a href="#">941019</a> AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:2523)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)