



# CVE-2023-0465

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-0465
<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>	2023-03-28 15:15:00 UTC
<b>Updated</b>	2024-02-04 09:15:00 UTC
<b>Description</b>	Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to

## Risk And Classification

**Problem Types:** CWE-295

## 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
<a href="http://www.openssl.org/news/secadv/20230328.txt">www.openssl.org/news/secadv/20230328.txt</a>	MISC	<a href="http://www.openssl.org">www.openssl.org</a>	
Debian -- Security Information -- DSA-5417-1 openssl	MISC	<a href="http://www.debian.org">www.debian.org</a>	
[SECURITY] [DLA 3449-1] openssl security update	MISC	<a href="http://lists.debian.org">lists.debian.org</a>	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		<a href="http://security.gentoo.org">security.gentoo.org</a>	
<a href="https://git.openssl.org">git.openssl.org</a> Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
<a href="https://git.openssl.org">git.openssl.org</a> Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
March 2023 OpenSSL Vulnerabilities in NetApp Products   NetApp Product Security	MISC	<a href="http://security.netapp.com">security.netapp.com</a>	
<a href="https://git.openssl.org">git.openssl.org</a> Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
<a href="https://git.openssl.org">git.openssl.org</a> Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">160752</a> Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-3722)
<a href="#">181818</a> Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5417-1)
<a href="#">181834</a> Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3449-1)
<a href="#">183838</a> Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0465)
<a href="#">241736</a> Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:3722)
<a href="#">242553</a> Red Hat Update for JBoss Core Services (RHSA-2023:7625)
<a href="#">330149</a> IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory39)
<a href="#">355097</a> Amazon Linux Security Advisory for openssl11 : ALAS2-2023-2039
<a href="#">355167</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-181
<a href="#">355387</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2023-2073
<a href="#">355428</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2023-1762
<a href="#">355523</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2023-422
<a href="#">356233</a> Amazon Linux Security Advisory for openssl-snapsafe : ALASOPENSSL-SNAPSAFE-2023-002
<a href="#">356483</a> Amazon Linux Security Advisory for openssl-snapsafe : ALAS2OPENSSL-SNAPSAFE-2023-002
<a href="#">357333</a> Amazon Linux Security Advisory for edk2 : ALAS2-2024-2502
<a href="#">379141</a> SolarWinds Serv-U HTML Injection Vulnerability
<a href="#">38893</a> OpenSSL Invalid certificate policies
<a href="#">502694</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">502695</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">502696</a> Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)
<a href="#">502759</a> Alpine Linux Security Update for openssl
<a href="#">502909</a> Alpine Linux Security Update for openssl1.1-compat
<a href="#">503022</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">503119</a> Alpine Linux Security Update for openssl
<a href="#">505786</a> Alpine Linux Security Update for openssl1.1-compat
<a href="#">505904</a> Alpine Linux Security Update for openssl
<a href="#">672941</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1807)

<a href="#">672943</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1825)
<a href="#">673062</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2195)
<a href="#">673095</a> EulerOS Security Update for compat-openssl10 (EulerOS-SA-2023-2187)
<a href="#">673173</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2317)
<a href="#">673178</a> EulerOS Security Update for shim (EulerOS-SA-2023-2324)
<a href="#">673200</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2337)
<a href="#">673205</a> EulerOS Security Update for shim (EulerOS-SA-2023-2344)
<a href="#">673231</a> EulerOS Security Update for shim (EulerOS-SA-2023-2369)
<a href="#">673243</a> EulerOS Security Update for shim (EulerOS-SA-2023-2395)
<a href="#">673331</a> EulerOS Security Update for shim (EulerOS-SA-2023-2711)
<a href="#">673398</a> EulerOS Security Update for linux-sgx (EulerOS-SA-2023-3047)
<a href="#">673566</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2702)
<a href="#">673605</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2660)
<a href="#">673724</a> EulerOS Security Update for shim (EulerOS-SA-2024-1299)
<a href="#">674033</a> EulerOS Security Update for shim (EulerOS-SA-2023-2669)
<a href="#">691102</a> Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (425b9538-ce5f-11ed-ade3-d4c9ef517024)
<a href="#">691183</a> Free Berkeley Software Distribution (FreeBSD) Security Update for python (d86becfe-05a4-11ee-9d4a-080027eda32c)
<a href="#">710857</a> Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)
<a href="#">753896</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1790-1)
<a href="#">753898</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1794-1)
<a href="#">753923</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:1908-1)
<a href="#">753924</a> SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:1912-1)
<a href="#">753927</a> SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:1922-1)
<a href="#">754004</a> SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:1914-1)
<a href="#">906787</a> Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (25951-1)
<a href="#">906849</a> Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (25937-1)
<a href="#">907019</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kata-containers-cc (27241-1)
<a href="#">907543</a> Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31145-1)

© [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](#)