



# CVE-2022-4450

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

## Summary

<b>CVE</b>	CVE-2022-4450
<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>	2023-02-08 20:15:00 UTC
<b>Updated</b>	2024-02-04 09:15:00 UTC
<b>Description</b>	The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"),

## Risk And Classification

**Problem Types:** CWE-415

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Stormshield</a>	<a href="#">Stormshield Network Security</a>	All	All	All	All

## References

Reference	Source	Link	Tags
git.openssl.org Git - openssl.git/commitdiff	MISC	<a href="#">git.openssl.org</a>	
www.openssl.org/news/secadv/20230207.txt	MISC	<a href="#">www.openssl.org</a>	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		<a href="#">security.gentoo.org</a>	
git.openssl.org Git - openssl.git/commitdiff	MISC	<a href="#">git.openssl.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160481](#) Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-0946)

[160492](#) Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12152)

160521 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-1405)
160523 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12213)
160621 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-2165)
160668 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-2932)
161209 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-13026)
161210 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-13024)
161212 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-32791)
161213 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-13025)
161214 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-13027)
161215 Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-32790)
181546 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5343-1)
181593 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3325-1)
182673 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-4450)
199150 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5844-1)
200021 Ubuntu Security Notification for Node.js Vulnerabilities (USN-6564-1)
241227 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:0946)
241256 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1199)
241285 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1405)
241469 Red Hat Update for edk2 security (RHSA-2023:2165)
241496 Red Hat Update for edk2 (RHSA-2023:2932)
241568 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:3408)
241574 Red Hat Update for JBoss Core Services (RHSA-2023:3354)
283694 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-57f33242bc)
283709 Fedora Security Update for edk2 (FEDORA-2023-e1ffb79ddf)
283736 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-a5564c0a3f)
283759 Fedora Security Update for edk2 (FEDORA-2023-e821b64a4c)
330133 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory38)
354735 Amazon Linux Security Advisory for Open Secure Sockets Layer11 (OpenSSL11) : ALAS2-2023-1934
355000 Amazon Linux Security Advisory for Open Secure Sockets Layer11 (OpenSSL11) : ALAS2-2023-1934

<a href="#">355230</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-101
<a href="#">357333</a> Amazon Linux Security Advisory for edk2 : ALAS2-2024-2502
<a href="#">378416</a> Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2023:0033)
<a href="#">378491</a> NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Multiple OpenSSL Denial of Service (DoS) Vulnerabilities (NTAP-20230214-0011)
<a href="#">378515</a> Alibaba Cloud Linux Security Update for edk2 (ALINUX3-SA-2023:0044)
<a href="#">38894</a> Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities
<a href="#">43991</a> Hewlett Packard Enterprise (HPE) ArubaOS Multiple Vulnerabilities (ARUBA-PSA-2023-001)
<a href="#">502652</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">502653</a> Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)
<a href="#">502757</a> Alpine Linux Security Update for openssl
<a href="#">502907</a> Alpine Linux Security Update for openssl1.1-compat
<a href="#">505784</a> Alpine Linux Security Update for openssl1.1-compat
<a href="#">672879</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1602)
<a href="#">672984</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1875)
<a href="#">673006</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1850)
<a href="#">673018</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1982)
<a href="#">673042</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1960)
<a href="#">673086</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL)111d (EulerOS-SA-2023-2162)
<a href="#">673136</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2299)
<a href="#">673156</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2275)
<a href="#">673398</a> EulerOS Security Update for linux-sgx (EulerOS-SA-2023-3047)
<a href="#">691051</a> Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (648a432c-a71f-11ed-86e9-d4c9ef517024)
<a href="#">710857</a> Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)
<a href="#">730818</a> IBM MQ Appliance Multiple Security Vulnerabilities (6986567)
<a href="#">753636</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0310-1)
<a href="#">753640</a> SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:0312-1)
<a href="#">753647</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0311-1)
<a href="#">753649</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0309-1)

905442 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13311)
905450 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13332)
905455 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13323)
905459 Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13318)
905468 Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13347)
905469 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13351)
905483 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13323-1)
905538 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13351-1)
906765 Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13347-1)
940941 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:0946)
940962 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:1405)
941044 AlmaLinux Security Update for edk2 (ALSA-2023:2165)
941103 AlmaLinux Security Update for edk2 (ALSA-2023:2932)
960886 Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2023:1405)
960889 Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2023:0946)

© [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](#)**