



# CVE-2023-0217

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-0217  |
| <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>     | An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by |

## 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                |
|--|---------|--|---------------------|
| <a href="http://www.openssl.org/news/secadv/20230207.txt">www.openssl.org/news/secadv/20230207.txt</a> | MISC    | <a href="http://www.openssl.org">www.openssl.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/-/commitdiff">git.openssl.org Git - openssl.git/commitdiff</a>    | 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

[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)

[182340](#) Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0217)

[199150](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5844-1)

|        |  |
|--------|--|
| 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)  |
| 283694 | Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-57f33242bc)                                    |
| 283736 | Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-a5564c0a3f)                                    |
| 330133 | IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory38) |
| 355230 | Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-101                                 |
| 38894  | Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities   |
| 502653 | Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)   |
| 502757 | Alpine Linux Security Update for openssl   |
| 710857 | Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)                                 |
| 753640 | SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:0312-1)  |
| 940941 | AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:0946)   |
| 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](#)