



# CVE-2019-1552

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

## Summary

<b>CVE</b>	CVE-2019-1552
<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>	2019-07-30 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:08:00 UTC
<b>Description</b>	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verific

## Risk And Classification

**Problem Types:** CWE-295

## 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="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All

## References

### Reference

myF5

[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists

git.openssl.org Git - openssl.git/commitdiff

[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists

Oracle Critical Patch Update Advisory - July 2020

[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®

Oracle Critical Patch Update Advisory - October 2020

git.openssl.org Git - openssl.git/commitdiff

support.f5.com/csp/article/K94041354

Security Bulletin - Policy Auditor update fixes multiple vulnerabilities in third-party libraries (CVE-2016-0718, CVE-2016-4472, CVE-2016-5300)

git.openssl.org Git - openssl.git/commitdiff

support.f5.com/csp/article/K94041354

[R1] Nessus Network Monitor 5.11.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable@

[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists

www.openssl.org/news/secadv/20190730.txt

git.openssl.org Git - openssl.git/commitdiff

git.openssl.org Git - openssl.git/commitdiff

VU#429301 - Veritas Backup Exec is vulnerable to privilege escalation due to OPENSLLDIR location

cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf

[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists

git.openssl.org Git - openssl.git/commitdiff

Oracle Critical Patch Update - October 2019

Oracle Critical Patch Update Advisory - January 2020

Oracle Critical Patch Update Advisory - April 2020

CVE-2019-1552 OpenSSL Vulnerability in NetApp Products | NetApp Product Security

git.openssl.org Git - openssl.git/commitdiff

git.openssl.org Git - openssl.git/commitdiff

CVE Program record

NVD vulnerability detail



### Vendor Comments And Credit

Discovery Credit

**LEGACY:** Rich Mirch

### Legacy QID Mappings

[296078](#) Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)

[591280](#) Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

© 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](#).

