



# CVE-2018-16395

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

## Summary

<b>CVE</b>	CVE-2018-16395
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-16 18:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	An issue was discovered in the OpenSSL library in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.4	All	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	2.6.0	preview1	All	All

Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	2.6.0	preview2	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	2.6.0	preview1	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	2.6.0	preview2	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	All	All	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	All	All	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	All	All	All	All

## References

### Reference

[Red Hat Customer Portal](#)

[Debian -- Security Information -- DSA-4332-1 ruby2.3](#)

[USN-3808-1: Ruby vulnerabilities | Ubuntu security notices](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Ruby 2.5.2 Released](#)

[\[SECURITY\] \[DLA 1558-1\] ruby2.1 security update](#)

[Ruby 2.3.8 Released](#)

[Ruby OpenSSL::X509::Name\(\) May Fail to Prevent Remote Users from Bypassing Security Restrictions on the Target System - SecurityTrack](#)

[Red Hat Customer Portal](#)

[Ruby 2.4.5 Released](#)

[CVE-2018-16395: OpenSSL::X509::Name equality check does not work correctly](#)

[HackerOne](#)

[November 2018 Ruby Vulnerabilities in NetApp Products | NetApp Product Security](#)

[\[security-announce\] openSUSE-SU-2019:1771-1: important: Security update](#)

[Oracle Critical Patch Update Advisory - January 2020](#)

[Red Hat Customer Portal](#)

[Ruby 2.6.0-preview3 Released](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[296091 Oracle Solaris 11.4 Support Repository Update \(SRU\) 6.1.4 Missing \(CPUJAN2019\)](#)

500611 Alpine Linux Security Update for ruby

504371 Alpine Linux Security Update for ruby

690286 Free Berkeley Software Distribution (FreeBSD) Security Update for ruby (afc60484-0652-440e-b01a-5ef814747f06)

900014 CBL-Mariner Linux Security Update for openssl 1.1.1g

903209 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (2687)

© [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](#)**