



# CVE-2015-8960

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

## Summary

<b>CVE</b>	CVE-2015-8960
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-09-21 02:59:00 UTC
<b>Updated</b>	2023-01-30 17:33:00 UTC
<b>Description</b>	The TLS protocol 1.2 and earlier supports the rsa_fixed_dh, dss_fixed_dh, rsa_fixed_ecdh, and ecdsa_fixed_ecdh values for

## Risk And Classification

**Problem Types:** CWE-295

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apple</a>	<a href="#">Safari</a>	-	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Safari</a>	All	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Safari</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	-	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All
Application	<a href="#">IETF</a>	<a href="#">Transport Layer Security</a>	All	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Internet Explorer</a>	-	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Internet Explorer</a>	All	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Internet Explorer</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	-	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Clustered Data Ontap Antivirus Connector</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Data Ontap Edge</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Host Agent</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Shift</a>	-	All	All	All

Application	Netapp	Plug-in For Symantec Netbackup	-	All	All	All
Application	Netapp	Smi-s Provider	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapmanager	-	All	All	All
Application	Netapp	Snapmanager	-	All	All	All
Application	Netapp	Snapprotect	-	All	All	All
Application	Netapp	Snap Creator Framework	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	System Setup	-	All	All	All
Application	Opera	Opera	All	All	All	All
Application	Opera	Opera	All	All	All	All
Application	Opera	Opera Browser	-	All	All	All

## References

### Reference

TLS CVE-2015-8960 Man in the Middle Security Bypass Vulnerability

KCI Attacks against TLS

oss-security - Re: Possible CVE for TLS protocol issue

[www.usenix.org/system/files/conference/woot15/woot15-paper-hlauschek.pdf](http://www.usenix.org/system/files/conference/woot15/woot15-paper-hlauschek.pdf)

CVE-2015-8960 TLS Vulnerability in NetApp Products | NetApp Product Security

Matthew Green on Twitter: "This attack is hilarious. Install a client cert in a browser, MITM any connection it makes to certain servers. <https://t.co/...>

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**