CVE-2015-8960

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	-	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Google	Chrome	-	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Ietf	Transport Layer Security	All	All	All	All
Application	Microsoft	Internet Explorer	-	All	All	All
Application	Microsoft	Internet Explorer	All	All	All	All
Application	Microsoft	Internet Explorer	All	All	All	All
Application	Mozilla	Firefox	-	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Netapp	Clustered Data Ontap Antivirus Connector	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Host Agent	-	All	All	All
Application	Netapp	Oncommand Shift	-	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
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.
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.