CVE-2016-9574

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-9574
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-19 13:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	nss before version 3.30 is vulnerable to a remote denial of service during the session handshake when using SessionTicket

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Network Security Services	All	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All

References

Reference
1320695 - Enable use of session ticket keys if server has no RSA key pair
1404568 – (CVE-2016-9574) CVE-2016-9574 nss: Remote DoS during session handshake when using SessionTicket extention and ECDHE-
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report