CVE-2016-4925

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

Summary

CVE	CVE-2016-4925
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-13 17:29:00 UTC
Updated	2019-10-09 23:18:00 UTC
Description	Receipt of a specifically malformed IPv6 packet processed by the router may trigger a line card reset: processor exception (

Risk And Classification

Problem Types: CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junose	All	All	All	All
Operating System	Juniper	Junose	All	All	All	All
Operating System	Juniper	Junose	All	All	All	All
Operating System	Juniper	Junose	All	All	All	All

References

Reference
Juniper JunosE CVE-2016-4925 Denial of Service Vulnerability
Juniper JUNOSe IPv6 Processing Flaw Lets Remote Users Cause the Target Line Card to Restart - SecurityTracker
2016-10 Security Bulletin: JUNOSe: Line Card Reset: processor exception 0x68616c74 (halt) task: scheduler, upon receipt of crafted IPv6 pac
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