CVE-2018-0369

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

Summary

CVE	CVE-2018-0369
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-16 17:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the reassembly logic for fragmented IPv4 packets of Cisco StarOS running on virtual platforms could allow

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 5000	-	All	All	All
Hardware	Cisco	Asr 5000	-	All	All	All
Hardware	Cisco	Asr 5500	-	All	All	All
Hardware	Cisco	Asr 5500	-	All	All	All
Hardware	Cisco	Asr 5700	-	All	All	All
Hardware	Cisco	Asr 5700	-	All	All	All
Operating System	Cisco	Staros	All	All	All	All
Operating System	Cisco	Staros	All	All	All	All

References

Reference	Source	Link	Tags
Cisco StarOS for ASR 5000 Series Routers CVE-2018-0369 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Pa
Cisco StarOS IPv4 Fragmentation Denial of Service Vulnerability	CONFIRM	tools.cisco.com	Vendor A
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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**