CVE-2014-0684

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

Summary

CVE	CVE-2014-0684
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-07 10:55:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco NX-OS 6.2(2) on Nexus 7000 switches allows local users to cause a denial of service via crafted sed input, aka Bug I

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:S/C:N/I:N/A:C

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Complete

AV:L/AC:L/Au:S/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 7000	-	All	All	All

Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Operating System	Cisco	Nx-os	6.2\(2\)	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
Cisco Nexus 7000 Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	tools.cisco.com	Vendor Advisory
Cisco Nexus 7000 Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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