CVE-2014-0676

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

Summary

CVE	CVE-2014-0676
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-22 21:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco NX-OS allows local users to bypass intended TACACS+ command restrictions via a series of multiple commands, ak

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

EPSS: 0.000840000 probability, percentile 0.243110000 (date 2026-05-03)

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Operating System	Cisco	Nx-os	-	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Cisco NX-OS Software TACACS+ Server Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da
Cisco NX-OS Lets Local Users Bypass TACACS+ Authorization to Execute Commands - SecurityTracker	af854a3a-2127-422b-91ae-364da
osvdb.org/102366	af854a3a-2127-422b-91ae-364da
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da
Cisco Security Notice: Cisco NX-OS Software TACACS+ Command Authorization Vulnerability	af854a3a-2127-422b-91ae-364da
Security Advisory SA56597 - Cisco NX-OS TACACS+ Security Bypass Security Issue - Secunia	af854a3a-2127-422b-91ae-364da
Alert Details - Security Center - Cisco Systems	af854a3a-2127-422b-91ae-364da
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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