

CVE-2017-6649

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

Summary	
CVE	CVE-2017-6649
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-22 01:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	A vulnerability in the CLI of Cisco NX-OS System Software 7.1 through 7.3 running on Cisco Nexus Series Switches could allow an attacker to execute arbitrary commands with root privileges.

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-20 | CWE-77 | CWE-20 CWE-20

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	4.6		AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown	
Attack Vector	Local
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 5548up	-	All	All	All
Hardware	Cisco	Nexus 5596t	-	All	All	All
Hardware	Cisco	Nexus 5596up	-	All	All	All
Hardware	Cisco	Nexus 56128p	-	All	All	All
Hardware	Cisco	Nexus 5624q	-	All	All	All
Hardware	Cisco	Nexus 5648q	-	All	All	All
Hardware	Cisco	Nexus 5672up	-	All	All	All
Hardware	Cisco	Nexus 5672up-16g	-	All	All	All
Hardware	Cisco	Nexus 5696q	-	All	All	All
Operating System	Cisco	Nx-os	7.1\{1\}n1\{1\}	All	All	All
Operating System	Cisco	Nx-os	7.1\{2\}n1\{1\}	All	All	All
Operating System	Cisco	Nx-os	7.1\{3\}n1\{1\}	All	All	All
Operating System	Cisco	Nx-os	7.1\{3\}n1\{2.1\}	All	All	All
Operating System	Cisco	Nx-os	7.1\{3\}n1\{2\}	All	All	All
Operating System	Cisco	Nx-os	7.1\{3\}n1\{3.12\}	All	All	All
Operating System	Cisco	Nx-os	7.1\{4\}n1\{1\}	All	All	All
Operating System	Cisco	Nx-os	7.2\{0\}d1\{0.437\}	All	All	All

Operating System	Cisco	Nx-os	7.2\0)n1\1\	All	All	All
Operating System	Cisco	Nx-os	7.2\0)zz\99.1\	All	All	All
Operating System	Cisco	Nx-os	7.2\1)n1\1\	All	All	All
Operating System	Cisco	Nx-os	7.3\0)n1\1\	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	Cisco Nexus Series Switches	affected Cisco Nexus Series Switches		Not specified	

References						
Reference						So
Cisco Nexus Series Switches CLI Command Injection Vulnerability						af8
Multiple Cisco Products CVE-2017-6649 Local Command Injection Vulnerability						af8
Cisco Nexus 5000 Series Switches Input Validation Flaw Lets Local Users Read and Write Files on the Target System - SecurityTracker						af8
CVE Program record						CV
NVD vulnerability detail						NV

No vendor comments have been submitted for this CVE.

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