CVE-2014-7989

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

Summary

CVE	CVE-2014-7989
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-07 11:55:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco Unified Computing System on B-Series blade servers allows local users to gain shell privileges via a crafted (1) ping6

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

Problem Types: CWE-20 | 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
Hardware	Cisco	B200 M3	-	All	All	All

Hardware	Cisco	B200 M4	-	All	All	All
Hardware	Cisco	B22 M3	-	All	All	All
Hardware	Cisco	B230 M2	-	All	All	All
Hardware	Cisco	B260 M4	-	All	All	All
Hardware	Cisco	B420 M3	-	All	All	All
Hardware	Cisco	B440 M2	-	All	All	All
Hardware	Cisco	B460 M4	-	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sourc
Cisco Unified Computing System CVE-2014-7989 Multiple Local Privilege Escalation Vulnerabilities	af854a
Cisco Unified Computing System ping6 and traceroute6 Command Bugs Let Local Users Gain Elevated Privileges - SecurityTracker	af854a
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-7989	af854a
IBM X-Force Exchange	af854a
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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