CVE-2015-0582

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

Summary

CVE	CVE-2015-0582
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-10 02:59:43 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The High Availability (HA) subsystem in Cisco NX-OS on MDS 9000 devices allows remote attackers to cause a denial of s

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Mds 9000	All	All	All	All

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
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2015-0582	af854a3a-2127-422b-91ae-3
Cisco MDS 9000 NX-OS Software CVE-2015-0582 Denial of Service Vulnerability	af854a3a-2127-422b-91ae-3
Cisco MDS 9000 NX-OS High Availability Subsystem Flaw Lets Remote Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-3
IBM X-Force Exchange	af854a3a-2127-422b-91ae-3
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.