CVE-2015-0686

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

Summary

CVE	CVE-2015-0686
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-03 02:00:00 UTC
Updated	2015-09-29 19:29:00 UTC
Description	The SNMP implementation in Cisco NX-OS 6.1(2)I2(3) on Nexus 9000 devices, when a Reset High Availability (HA) policy

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 93120tx	-	All	All	All
Hardware	Cisco	Nexus 93120tx	-	All	All	All
Hardware	Cisco	Nexus 93128tx	-	All	All	All
Hardware	Cisco	Nexus 93128tx	-	All	All	All
Hardware	Cisco	Nexus 9332pq	-	All	All	All
Hardware	Cisco	Nexus 9332pq	-	All	All	All
Hardware	Cisco	Nexus 9336pq Aci Spine	-	All	All	All
Hardware	Cisco	Nexus 9336pq Aci Spine	-	All	All	All
Hardware	Cisco	Nexus 9372px	-	All	All	All
Hardware	Cisco	Nexus 9372px	-	All	All	All
Hardware	Cisco	Nexus 9372tx	-	All	All	All
Hardware	Cisco	Nexus 9372tx	-	All	All	All
Operating System	Cisco	Nx-os	6.1(2)i2(3)	All	All	All
Operating System	Cisco	Nx-os	6.1\(2\)i2\(3\)	All	All	All
Operating System	Cisco	Nx-os	6.1\(2\)i2\(3\)	All	All	All

References

Reference	Source	Link
Cisco Nexus 9000 SNMP Subsystem Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	SECTRACK	www.securitytr
Cisco Nexus 9000 Series Denial of Service Vulnerability	CISCO	tools.cisco.con
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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