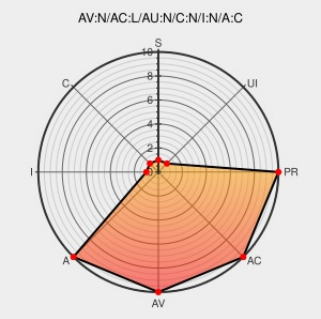
CVE-2009-0627

Published on: 09/08/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:29 PM UTC

CVE-2009-0627

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nexus 5000 from Cisco contain the following vulnerability:

Unspecified vulnerability in Cisco NX-OS before 4.0(1a)N2(1), when running on Nexus 5000 platforms, allows remote attackers to cause a denial of service (crash) via an unspecified "sequence of TCP packets" related to "TCP State manipulation," possibly related to separate attacks against CVE-2008-4609.

CVE-2009-0627 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco Security Advisory: TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products - Cisco Systems	Patch, Vendor Advisory, www.cisco.com, text/html	CISCO 20090908 TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products
SecurityTracker.com Archives - Cisco NX-OS TCP Processing Bug Lets Remote Users Deny Service	www.securitytracker.com, text/html	SECTRACK 1022847

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 5000	All	All	All	All
Hardware	Cisco	Nexus 5000	All	All	All	All
Hardware	Cisco	Nexus 7000	All	All	All	All
Hardware	Cisco	Nexus 7000	All	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All

cpe:2.3:h:cisco:nexus_5000:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5000:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_7000:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_7000:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→