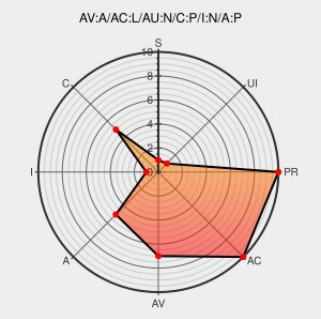
CVE-2015-6295

Published on: 09/20/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6295

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



Certain versions of Nexus 9000 from Cisco contain the following vulnerability:

Cisco NX-OS 6.1(2)I3(4) and 7.0(3)I1(1) on Nexus 9000 (N9K) devices allows remote attackers to cause a denial of service (CPU consumption or control-plane instability) or trigger unintended traffic forwarding via a Layer 2 packet with a reserved VLAN number, aka Bug ID CSCuw13560.

CVE-2015-6295 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 4.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco NX-OS VLAN Processing Flaw Lets Remote Users on the Local Network Consume Excessive CPU Resources on the Target System - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1033611
Cisco Nexus 9000 Series Switches Reserved VLAN Number Vulnerability	Vendor Advisory, tools.cisco.com, text/html	CISCO 20150916 Cisco Nexus 9000 Series Switches Reserved VLAN Number Vulnerability

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 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)i3(4)	All	All	All
Operating System	Cisco	Nx-os	6.1\(2\)i3\(4\)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i1(1)	All	All	All
Operating System	Cisco	Nx-os	7.0\(3\)i1\(1\)	All	All	All
Operating System	Cisco	Nx-os	6.1\(2\)i3\(4\)	All	All	All
Operating System	Cisco	Nx-os	7.0\(3\)i1\(1\)	All	All	All

cpe:2.3:h:cisco:nexus_9000:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9000:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_93120tx:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_93120tx:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_93128tx:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_93128tx:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9332pq:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9332pq:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9336pq_aci_spine:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9336pq_aci_spine:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9372px:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9372px:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9372tx:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_9372tx:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:6.1(2)i3(4):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:6.1\(2\)i3\(4\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:7.0(3)i1(1):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:7.0\(3\)i1\(1\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:6.1\(2\)i3\(4\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:7.0\(3\)i1\(1\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→