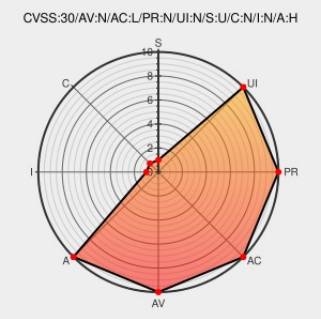
CVE-2015-6260

Published on: 03/03/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6260

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



Certain versions of Nexus 5548p from Cisco contain the following vulnerability:

Cisco NX-OS 7.1(1)N1(1) on Nexus 5500, 5600, and 6000 devices does not properly validate PDUs in SNMP packets, which allows remote attackers to cause a denial of service (SNMP application restart) via a crafted packet, aka Bug ID CSCut84645.

CVE-2015-6260 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

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 Nexus 5500/5600/6000 Switches SNMP Input Validation Flaw Lets Remote Users Cause the Target System to Crash - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1035158
Cisco NX-OS Software SNMP Packet Denial of Service Vulnerability	Vendor Advisory tools.cisco.com	CISCO 20160302 Cisco NX-OS Software SNMP Packet Denial of

text/html Service Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 5548p	-	All	All	All
Hardware	Cisco	Nexus 5548p	-	All	All	All
Hardware	Cisco	Nexus 5548up	-	All	All	All
Hardware	Cisco	Nexus 5548up	-	All	All	All
Hardware	Cisco	Nexus 5596t	-	All	All	All
Hardware	Cisco	Nexus 5596t	-	All	All	All
Hardware	Cisco	Nexus 5596up	-	All	All	All
Hardware	Cisco	Nexus 5596up	-	All	All	All
Hardware	Cisco	Nexus 56128p	-	All	All	All
Hardware	Cisco	Nexus 56128p	-	All	All	All
Hardware	Cisco	Nexus 5624q	-	All	All	All
Hardware	Cisco	Nexus 5624q	-	All	All	All
Hardware	Cisco	Nexus 5648q	-	All	All	All
Hardware	Cisco	Nexus 5648q	-	All	All	All
Hardware	Cisco	Nexus 5672up	-	All	All	All
Hardware	Cisco	Nexus 5672up	-	All	All	All
Hardware	Cisco	Nexus 5696q	-	All	All	All
Hardware	Cisco	Nexus 5696q	-	All	All	All
Operating System	Cisco	Nx-os	7.1\(1\)n1\(1\)	All	All	All
Operating System	Cisco	Nx-os	7.1\\\(1\\\)n1\\\(1\\\)	All	All	All
Operating System	Cisco	Nx-os	7.1\\\(1\\\)n1\\\(1\\\)	All	All	All
Operating System	Zyxel	Gs1900-10hp Firmware	All	All	All	All

cpe:2.3:h:cisco:nexus_5548p:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5548p:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5548up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5548up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5596t:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5596t:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5596up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5596up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_56128p:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_56128p:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5624q:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5624q:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5648q:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5648q:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5672up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5672up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5696q:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:nexus_5696q:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:7.1\(1\)n1\(1\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:7.1\\\(1\\\)n1\\\(1\\\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:7.1\\\(1\\\)n1\\\(1\\\):*:*:*:*:*:*:*:

cpe:2.3:o:zyxel:gs1900-10hp_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report