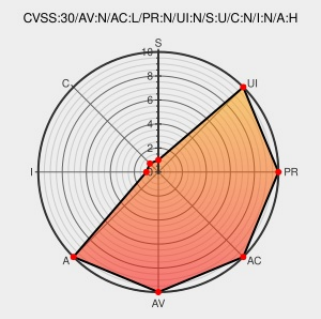
CVE-2015-6398

Published on: 02/07/2016 12:00:00 AM UTC

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

CVE-2015-6398

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



Certain versions of Nx-os from Cisco contain the following vulnerability:

Cisco Nexus 9000 Application Centric Infrastructure (ACI) Mode switches with software before 11.0(1c) allow remote attackers to cause a denial of service (device reload) via an IPv4 ICMP packet with the IP Record Route option, aka Bug ID CSCuq57512.

CVE-2015-6398 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 9000 Series ACI Mode Switch ICMP Record Route Vulnerability	Vendor Advisory, tools.cisco.com, text/html	CISCO 20160203 Cisco Nexus 9000 Series ACI Mode Switch ICMP Record Route Vulnerability
Cisco Nexus 9000 Series ACI Mode Switch Lets Remote Users	www.securitytracker.com	SECTRACK 1034928

Cause the Target System to Reload - SecurityTracker text/html

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
Operating System	Cisco	Nx-os	11.0\(1b\)	All	All	All
Operating System	Cisco	Nx-os	11.0\\\(1b\\\)	All	All	All
Operating System	Cisco	Nx-os	11.0\\\(1b\\\)	All	All	All
Operating System	Zyxel	Gs1900-10hp Firmware	All	All	All	All

cpe:2.3:o:cisco:nx-os:11.0\(1b\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\\\(1b\\\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\\\(1b\\\):*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID Next ID→