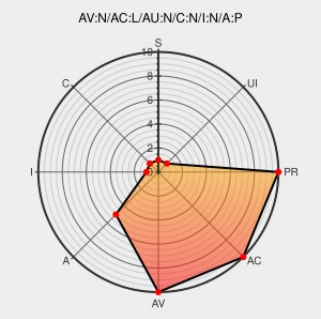
CVE-2014-3270

Published on: 05/20/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-3270

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



Certain versions of Ios Xr from Cisco contain the following vulnerability:

The DHCPv6 implementation in Cisco IOS XR allows remote attackers to cause a denial of service (process hang) via a malformed packet, aka Bug ID CSCul80924.

CVE-2014-3270 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory, tools.cisco.com, text/html	CISCO 20140519 Cisco IOS XR Software DHCP Version 6 Process Hang Vulnerability
Cisco IOS XR DHCPv6 Processing Flaw Lets Remote Users Deny Service - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1030259

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	Ios Xr	All	All	All	All
Operating System	Cisco	Ios Xr	All	All	All	All

cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→