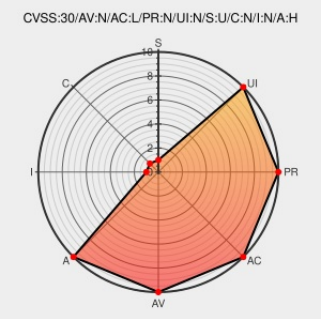
CVE-2016-9205

Published on: 12/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9205

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



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

A vulnerability in the HTTP 2.0 request handling code of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the Event Management Service daemon (emsd) to crash, resulting in a denial of service (DoS) condition. More Information: CSCvb14425. Known Affected Releases: 6.1.1.BASE. Known Fixed Releases: 6.1.2.6i.MGBL 6.1.22.9i.MGBL 6.2.1.14i.MGBL.

CVE-2016-9205 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: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco IOS XR Software HTTP 2.0 Request Handling Event Service Daemon Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios-xr

Cisco IOS XR Software CVE-2016-9205 Denial of Service Vulnerability

Third Party Advisory
VDB Entry
cve.report (archive)
text/html

BID 94813

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	6.1.1	All	All	All
Operating System	Cisco	Ios Xr	6.1.1	All	All	All

cpe:2.3:o:cisco:ios_xr:6.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→