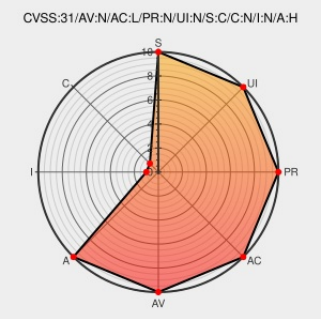
CVE-2020-3566

Published on: 08/29/2020 12:00:00 AM UTC

Last Modified on: 10/21/2022 07:48:00 PM UTC

CVE-2020-3566 - advisory for cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

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



Certain versions of Asr 9001 from Cisco contain the following vulnerability:

A vulnerability in the Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to exhaust process memory of an affected device. The vulnerability is due to insufficient queue management for Internet Group Management Protocol (IGMP) packets. An attacker could exploit this vulnerability by sending crafted IGMP traffic to an affected device. A successful exploit could allow the attacker to cause memory exhaustion, resulting in instability of other processes. These processes may include, but are not limited to, interior and exterior routing protocols. Cisco will release software updates that address this vulnerability.

CVE-2020-3566 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

On August 28, 2020, the Cisco Product Security Incident Response Team (PSIRT) became aware of attempted exploitation of this vulnerability in the wild. For affected products, Cisco recommends implementing a mitigation that is appropriate for the customer's environment.

Affected Vendor/Software: **Cisco** - **Cisco IOS XR Software** version **n/a**

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 IOS XR Software DVMRP Memory Exhaustion Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20200829 Cisco IOS XR Software DVMRP Memory Exhaustion 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	Asr 9001	-	All	All	All
Hardware	Cisco	Asr 9001	-	All	All	All
Hardware	Cisco	Asr 9006	-	All	All	All
Hardware	Cisco	Asr 9006	-	All	All	All
Hardware	Cisco	Asr 9010	-	All	All	All
Hardware	Cisco	Asr 9010	-	All	All	All
Hardware	Cisco	Asr 9901	-	All	All	All
Hardware	Cisco	Asr 9901	-	All	All	All
Hardware	Cisco	Asr 9904	-	All	All	All
Hardware	Cisco	Asr 9904	-	All	All	All
Hardware	Cisco	Asr 9906	-	All	All	All
Hardware	Cisco	Asr 9906	-	All	All	All
Hardware	Cisco	Asr 9910	-	All	All	All
Hardware	Cisco	Asr 9910	-	All	All	All
Hardware	Cisco	Asr 9912	-	All	All	All
Hardware	Cisco	Asr 9912	-	All	All	All
Hardware	Cisco	Asr 9922	-	All	All	All
Hardware	Cisco	Asr 9922	-	All	All	All

Operating System	Cisco	Ios Xr	6.4.2	All	All	All
Operating System	Cisco	Ios Xr	6.4.2	All	All	All

- cpe:2.3:h:cisco:asr_9001:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9001:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9006:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9006:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9010:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9010:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9901:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9901:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9904:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9904:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9906:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9906:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9910:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9910:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9912:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9912:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9922:-:*:*:*:*:*:*:*:
- cpe:2.3:h:cisco:asr_9922:-:*:*:*:*:*:*:*:
- cpe:2.3:o:cisco:ios_xr:6.4.2:*:*:*:*:*:*:*:
- cpe:2.3:o:cisco:ios_xr:6.4.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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