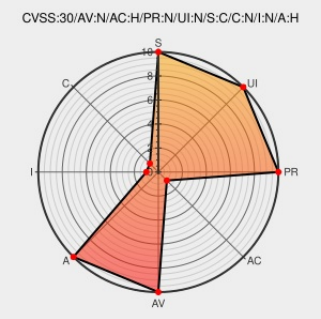
CVE-2018-15428

Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-15428 - advisory for cisco-sa-20181003-iosxr-dos

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



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

A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain BGP update messages. An attacker could exploit this vulnerability by sending BGP update messages that include a specific, malformed attribute to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic only from explicitly defined peers. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer, or would need to be injected by the attacker into the victim's BGP network on an existing, valid TCP connection to a BGP peer.

CVE-2018-15428 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS3 Score: 6.8 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco IOS XR Software Border Gateway Protocol Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20181003 Cisco IOS XR Software Border Gateway Protocol Denial of Service Vulnerability
Cisco IOS XR BGP Processing Error Lets Remote Users Cause the Target System to Reload - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041790

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	6.0.1	All	All	All
Operating System	Cisco	Ios Xr	6.0.2	All	All	All
Operating System	Cisco	Ios Xr	6.1.1	All	All	All
Operating System	Cisco	Ios Xr	6.1.2	All	All	All
Operating System	Cisco	Ios Xr	6.1.3	All	All	All
Operating System	Cisco	Ios Xr	6.1.4	All	All	All
Operating System	Cisco	Ios Xr	6.2.1	All	All	All
Operating System	Cisco	Ios Xr	6.2.2	All	All	All
Operating System	Cisco	Ios Xr	6.2.3	All	All	All
Operating System	Cisco	Ios Xr	6.4.1	All	All	All
Operating System	Cisco	Ios Xr	6.0.1	All	All	All
Operating System	Cisco	Ios Xr	6.0.2	All	All	All
Operating System	Cisco	Ios Xr	6.1.1	All	All	All
Operating System	Cisco	Ios Xr	6.1.2	All	All	All
Operating System	Cisco	Ios Xr	6.1.3	All	All	All
Operating System	Cisco	Ios Xr	6.1.4	All	All	All
Operating System	Cisco	Ios Xr	6.2.1	All	All	All
Operating System	Cisco	Ios Xr	6.2.2	All	All	All
Operating System	Cisco	Ios Xr	6.2.3	All	All	All
Operating System	Cisco	Ios Xr	6.4.1	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:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.0.2:*:*:*:*:*:*:*:

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

cpe:2.3:o:cisco:ios_xr:6.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.0.2:*:*:*:*:*:*:*:

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

cpe:2.3:o:cisco:ios_xr:6.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→