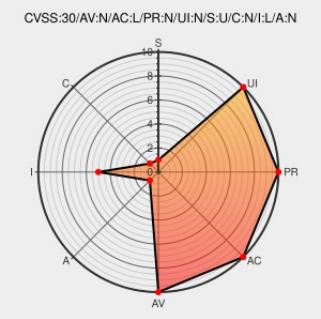
CVE-2019-15998

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15998 - advisory for cisco-sa-20191120-iosxr-ssh-bypass

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



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

A vulnerability in the access-control logic of the NETCONF over Secure Shell (SSH) of Cisco IOS XR Software may allow connections despite an access control list (ACL) that is configured to deny access to the NETCONF over SSH of an affected device. The vulnerability is due to a missing check in the NETCONF over SSH access control list (ACL). An attacker could exploit this vulnerability by connecting to an affected device using NETCONF over SSH. A successful exploit could allow the attacker to connect to the device on the NETCONF port. Valid credentials are required to access the device. This vulnerability does not affect connections to the default SSH process on the device.

CVE-2019-15998 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

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

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: 5 - MEDIUM

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

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco IOS XR Software NETCONF Over Secure Shell ACL Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20191120 Cisco IOS XR Software NETCONF Over Secure Shell ACL Bypass 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 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	6.5.1	All	All	All
Operating System	Cisco	Ios Xr	6.5.2	All	All	All
Operating System	Cisco	Ios Xr	6.5.3	All	All	All
Operating	Cisco	Ios Xr	6.5.1	All	All	All

System						
Operating System	Cisco	Ios Xr	6.5.2	All	All	All
Operating System	Cisco	Ios Xr	6.5.3	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_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:6.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:6.5.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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