



CVE-2019-15998

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

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

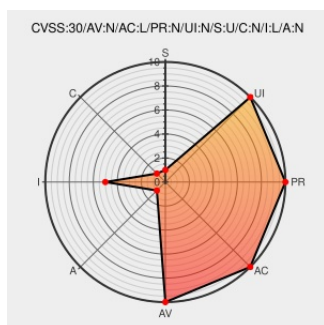
CVE-2019-15998 - advisory for cisco-sa-20191120-iosxr-ssh-bypass

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
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

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	los Xr	6.5.1	All	All	All
Operating System	Cisco	los Xr	6.5.2	All	All	All
Operating System	Cisco	los Xr	6.5.3	All	All	All
Operating	Cisco	los 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→

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)