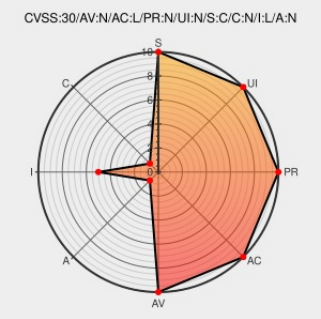
CVE-2020-3444

Published on: 11/06/2020 12:00:00 AM UTC

Last Modified on: 08/06/2021 07:01:00 PM UTC

CVE-2020-3444 - advisory for cisco-sa-cedge-filt-bypass-Y6wZMqm4

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



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

A vulnerability in the packet filtering features of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to bypass L3 and L4 traffic filters. The vulnerability is due to improper traffic filtering conditions on an affected device. An attacker could exploit this vulnerability by crafting a malicious TCP packet with specific characteristics and sending it to a targeted device. A successful exploit could allow the attacker to bypass the L3 and L4 traffic filters and inject an arbitrary packet into the network.

CVE-2020-3444 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH 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 SD-WAN Solution** 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	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco SD-WAN Software Packet Filtering Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201104 Cisco SD-WAN Software Packet Filtering 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

Exploit/POC from Github

PoC for exploiting CVE-2020-3444 : A vulnerability in the packet filtering features of Cisco SD-WAN Software could al…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ios Xe	All	All	All	All
Operating System	Cisco	Ios Xe	All	All	All	All
Application	Cisco	Ios Xe	All	All	All	All
Operating System	Cisco	Ios Xe	All	All	All	All

cpe:2.3:a:cisco:ios_xe:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ios_xe:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

© CVE.report 2023 | Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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 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