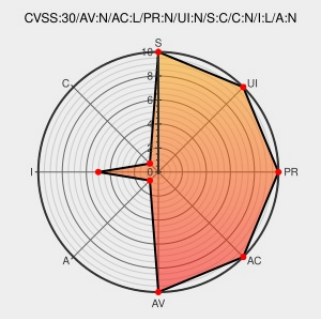
CVE-2020-3133

Published on: 09/22/2020 12:00:00 AM UTC

Last Modified on: 08/12/2021 06:19:00 PM UTC

CVE-2020-3133 - advisory for cisco-sa-esa-bypass-5Cdv2HMA

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



Certain versions of Email Security Appliance from Cisco contain the following vulnerability:

A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper validation of incoming emails. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass the configured content filters, which could allow malicious content to pass through the device.

CVE-2020-3133 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 Email Security Appliance (ESA)** 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 Email Security Appliance Content Filter Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200122 Cisco Email Security Appliance Content Filter 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
Application	Cisco	Email Security Appliance	All	All	All	All
Application	Cisco	Email Security Appliance	All	All	All	All

cpe:2.3:a:cisco:email_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:email_security_appliance:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→