



CVE-2019-1933

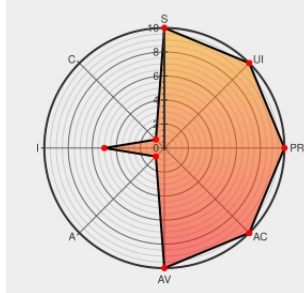
Published on: 07/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

CVE-2019-1933 - advisory for cisco-sa-20190703-esa-filterpass

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N



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 input validation of certain email fields. 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 configured message filters and inject arbitrary scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.

CVE-2019-1933 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 **11.1.2-023**

CVSS3 Score: **7.4 - HIGH**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	Integrity	Availability

Impact

NONE

Impact

PARTIAL

Impact

NONE

CVE References

Description	Tags	Link
Cisco Email Security Appliance Content Filter Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20190703 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	11.1.2-023	All	All	All
Application	Cisco	Email Security Appliance	11.1.2-023	All	All	All

cpe:2.3:a:cisco:email_security_appliance:11.1.2-023:*:*:*:*:*:

cpe:2.3:a:cisco:email_security_appliance:11.1.2-023:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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 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](#)