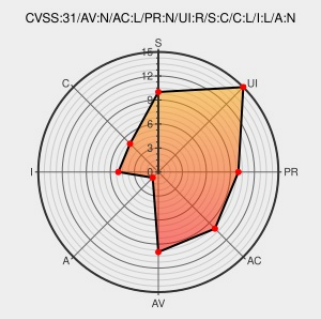
CVE-2020-3599

Published on: 10/21/2020 12:00:00 AM UTC

Last Modified on: 08/16/2023 04:17:00 PM UTC

CVE-2020-3599 - advisory for cisco-sa-asa-rxss-L54Htxp

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



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

A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.

CVE-2020-3599 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 Adaptive Security Appliance (ASA) Software** version **n/a**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Adaptive Security Appliance Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Adaptive Security Appliance Software Web-Based Management Interface Reflected Cross-Site Scripting 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	Adaptive Security Appliance	All	All	All	All
Application	Cisco	Adaptive Security Appliance	All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All

cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→