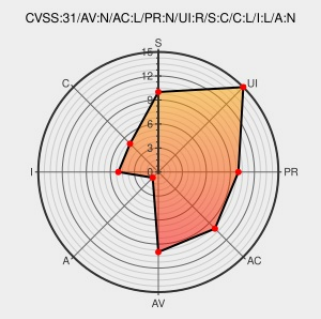
CVE-2020-3583

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

Last Modified on: 05/26/2022 03:11:00 PM UTC

CVE-2020-3583 - advisory for cisco-sa-asaftd-xss-multiple-FCB3vPZe

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



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

Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities 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 allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.

CVE-2020-3583 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 vulnerabilities that are 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 Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Interface Cross-Site Scripting Vulnerabilities	Patch Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Interface Cross-Site Scripting Vulnerabilities

Related QID Numbers

150447 Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Cross-Site Scripting (XSS) Vulnerabilities

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Operating System	Cisco	Firepower Threat Defense	All	All	All	All
Operating System	Cisco	Firepower Threat Defense	All	All	All	All

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

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

cpe:2.3:o:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | Multiple vulnerabilities in the web serv... | CVE-2020-3583 | Link for more: alerts.remotelyrmm.com/CVE-2020-3583	2022-05-26 16:28:19

← Previous ID Next ID →