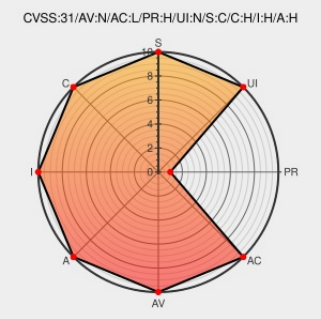
CVE-2022-20829

Published on: Not Yet Published

Last Modified on: 10/26/2022 07:46:00 PM UTC

CVE-2022-20829 - advisory for cisco-sa-asa-asdm-sig-NPKvwDjm

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



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

A vulnerability in the packaging of Cisco Adaptive Security Device Manager (ASDM) images and the validation of those images by Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker with administrative privileges to upload an ASDM image that contains malicious code to a device that is running Cisco ASA Software. This vulnerability is due to insufficient validation of the authenticity of an ASDM image during its installation on a device that is running Cisco ASA Software. An attacker could exploit this vulnerability by installing a crafted ASDM image on the device that is running Cisco ASA Software and then waiting for a targeted user to access that device using ASDM. A successful exploit could allow the attacker to execute arbitrary code on the machine of the targeted user with the privileges of that user on that machine. Notes: To successfully exploit this vulnerability, the attacker must have administrative privileges on the device that is running Cisco ASA Software. Potential targets are limited to users who manage the same device that is running Cisco ASA Software using ASDM. Cisco has released and will release software updates that address this vulnerability.

CVE-2022-20829 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

The Cisco 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: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
GitHub - jbaines-r7/theway: A tool for extracting, modifying, and crafting ASDM binary packages (CVE-2022-20829)	github.com text/html	MISC github.com/jbaines-r7/theway
Rapid7 Discovered Vulnerabilities in Cisco ASA, ASDM, and FirePOWER | Rapid7 Blog	www.rapid7.com text/html	MISC www.rapid7.com/blog/post/2022/08/11/rapid7-discovered-vulnerabilities-in-cisco-asa-asdm-and-firepower-services-software/
No Description Provided	tools.cisco.com text/html	CISCO 20220622 Cisco Adaptive Security Device Manager and Adaptive Security Appliance Software Client-side Arbitrary Code Execution Vulnerability

Related QID Numbers

317201 Cisco Adaptive Security Device Manager (ASDM) and Adaptive Security Appliance (ASA) Software Client-side Arbitrary Code Execution Vulnerability (cisco-sa-asa-asdm-sig-NPKvwDjm)

Exploit/POC from Github

A tool for extracting, modifying, and crafting ASDM binary packages (CVE-2022-20829)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Adaptive Security Device Manager	All	All	All	All
Hardware	Cisco	Asa 5512-x	-	All	All	All
Operating System	Cisco	Asa 5512-x Firmware	All	All	All	All
Hardware	Cisco	Asa 5515-x	-	All	All	All
Operating System	Cisco	Asa 5515-x Firmware	All	All	All	All
Hardware	Cisco	Asa 5585-x	-	All	All	All
Operating	Cisco	Asa 5585-x Firmware	All	All	All	All

System						
Hardware	Cisco	Firepower 1010	-	All	All	All
Hardware	Cisco	Firepower 1120	-	All	All	All
Hardware	Cisco	Firepower 1140	-	All	All	All
Hardware	Cisco	Firepower 1150	-	All	All	All
Hardware	Cisco	Firepower 2110	-	All	All	All
Hardware	Cisco	Firepower 2120	-	All	All	All
Hardware	Cisco	Firepower 2130	-	All	All	All
Hardware	Cisco	Firepower 2140	-	All	All	All
Hardware	Cisco	Firepower 4110	-	All	All	All
Hardware	Cisco	Firepower 4112	-	All	All	All
Hardware	Cisco	Firepower 4115	-	All	All	All
Hardware	Cisco	Firepower 4120	-	All	All	All
Hardware	Cisco	Firepower 4125	-	All	All	All
Hardware	Cisco	Firepower 4140	-	All	All	All
Hardware	Cisco	Firepower 4145	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Hardware	Cisco	Isa 3000	-	All	All	All
Operating System	Cisco	Isa 3000 Firmware	All	All	All	All

cpe:2.3:a:cisco:adaptive_security_device_manager:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:asa_5512-x:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:asa_5512-x_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:asa_5515-x:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:asa_5515-x_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:asa_5585-x:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:asa_5585-x_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_1010:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_1120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_1140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_1150:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2110:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2130:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4110:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4112:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4115:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4125:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4145:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_9300:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:isa_3000:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:isa_3000_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@sidfm_jp	Cisco ASA Software の ASDM の処理に任意のコードを実行される問題 (CVE-2022-20829) [42579] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2022-06-23 05:30:03
@RedPacketSec	Cisco Adaptive Security Device Manager and Adaptive Security Appliance Software code execution | CVE-2022-20829 -… twitter.com/i/web/status/1…	2022-06-24 09:01:05
@CVEreport	CVE-2022-20829 : A vulnerability in the packaging of Cisco Adaptive Security Device Manager ASDM images and the… twitter.com/i/web/status/1…	2022-06-24 15:28:37
/r/netcve	CVE-2022-20829	2022-06-24 16:38:23

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report