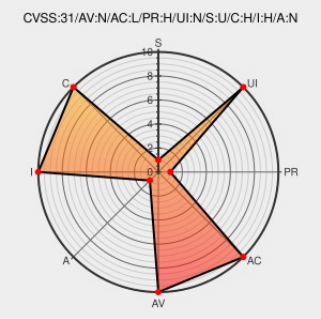
CVE-2022-20828

Published on: Not Yet Published

Last Modified on: 09/05/2022 05:15:00 PM UTC

CVE-2022-20828 - advisory for cisco-sa-asasfr-cmd-inject-PE4GfdG

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



Certain versions of Asa Firepower from Cisco contain the following vulnerability:

A vulnerability in the CLI parser of Cisco FirePOWER Software for Adaptive Security Appliance (ASA) FirePOWER module could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected ASA FirePOWER module as the root user. This vulnerability is due to improper handling of undefined command parameters. An attacker could exploit this vulnerability by using a crafted command on the CLI or by submitting a crafted HTTPS request to the web-based management interface of the Cisco ASA that is hosting the ASA FirePOWER module. Note: To exploit this vulnerability, the attacker must have administrative access to the Cisco ASA. A user who has administrative access to a particular Cisco ASA is also expected to have administrative access to the ASA FirePOWER module that is hosted by that Cisco ASA.

CVE-2022-20828 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 FirePOWER Services Software for ASA** 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
No Description Provided	tools.cisco.com text/html	CISCO 20220622 Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability
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/
Cisco ASA-X With FirePOWER Services Authenticated Command Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/168256/Cisco-ASA-X-With-FirePOWER-Services-Authenticated-Command-Injection.html

Related QID Numbers

317202 Cisco Firepower Software for ASA Firepower Module Command Injection Vulnerability (cisco-sa-asasfr-cmd-inject-PE4GfdG)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Asa Firepower	All	All	All	All
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 4150	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Hardware	Cisco	Firepower Management Center	-	All	All	All
Hardware	Cisco	Firepower Management Center Virtual Appliance	-	All	All	All

cpe:2.3:a:cisco:asa_firepower:*:*:*:*:*:*:*:*:

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_4150:-:*:*:*:*:*:*:*:

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

cpe:2.3:h:cisco:firepower_management_center:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_management_center_virtual_appliance:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@SystemTek_UK	Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability [CVE-2022-20828] systemtek.co.uk/2022/06/cisco-…	2022-06-23 12:55:11
@6townstechteam	Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability [CVE-2022-20828] systemtek.co.uk/2022/06/cisco-…	2022-06-23 12:55:13
@CVEreport	CVE-2022-20828 : A vulnerability in the CLI parser of Cisco FirePOWER Software for Adaptive Security Appliance A… twitter.com/i/web/status/1…	2022-06-24 15:32:27
/r/netcve	CVE-2022-20828	2022-06-24 16:38:24

← Previous ID

Next ID→