Advisory Alert

Alert Number: AAA20220623 **Date:** June 23, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Medium**	Multiple vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20828,CVE-2022-20829)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in the Cisco Cisco FirePOWER software and Cisco Adaptive Security Device Manager. **CVE-2022-20828** - Due to a vulnerability that exists in the CLI parser of Cisco FirePOWER Software for Adaptive Security Appliance (ASA) FirePOWER module it leads an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected ASA FirePOWER module as the root user. This is due to improper handling of undefined command parameters. It allows an attacker to 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. **CVE-2022-20829** - Due to a vulnerability that exists in the packaging of Cisco Adaptive Security Device Manager (ASDM) images and the validation of those images by Cisco Adaptive Security Appliance (ASA) Software leads 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. And this vulnerability is caused due to insufficient validation of the authenticity of an ASDM image during its installation on a device that is running Cisco ASA Software. It allows an attacker to 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. Successful exploitation could allow the attacker to execute arbitrary code on the machine of the targeted user with the privileges of that user on that machine. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Cisco FirePOWER Software for ASA FirePOWER Module 6.2.2 and earlier, 6.2.3, 6.3.0, 6.4.0, 6.5.0, 6.6.0, 6.7.0, 7.0 Cisco ASA Release 9.17 and earlier, 9.18 Cisco ASDM Release 7.17 and earlier, 7.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asasfr-cmd-inject-PE4GfdG https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.