TLP: WHITE

Advisory Alert

Alert Number: AAA20230504 **Date:** May 4, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Remote Command Execution Vulnerability
Fortinet	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Command Execution Vulnerability (CVE-2023-20126)
Description	Cisco has released a security update addressing a remote command execution vulnerability that exists in Cisco SPA112 2-Port Phone Adapters. **CVE-2023-20126** - This is a vulnerability that exists in the web-based management interface of Cisco SPA112 2-Port Phone Adapters due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with full privileges. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All firmware releases for Cisco SPA112 2-Port Phone Adapters.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW

Affected Product	**Fortinet**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27999, CVE-2023-27993, CVE-2022-45858, CVE-2023-22637, CVE-2022-45860, CVE-2022-45859, CVE-2023-26203, CVE-2022-43950, CVE-2023-22640)	
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to unauthorized commands and code execution, arbitrary directory deletion, sensitive information disclosure, user redirection to malicious websites, and attacker to carry out password spraying attacks. Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.	
Affected Products	FortiADC version 7.2.0 FortiADC version 7.1.0 through 7.1.1 FortiADC 7.0 all versions FortiADC 6.2 all versions FortiADC 6.1 all versions FortiADC 6.0 all versions FortiADC 5.4 all versions FortiADC 5.3 all versions FortiADC 5.2 all versions FortiNAC-F version 7.2.0 FortiNAC version 9.2.0 through 9.2.6 FortiNAC version 9.1.0 through 9.1.8 FortiNAC version 8.8.0 through 8.8.11	FortiNAC version 8.7.0 through 8.7.6 FortiNAC version 9.4.0 through 9.4.2 FortiNAC 9.2 all versions FortiNAC 9.1 all versions FortiNAC 8.8 all versions FortiNAC 8.7 all versions FortiOS version 7.2.0 through 7.2.3 FortiOS version 7.0.0 through 7.0.10 FortiOS version 6.4.0 through 6.4.11 FortiOS version 6.2.0 through 6.2.13 FortiOS 6.0 all versions FortiProxy version 7.2.0 through 7.2.1 FortiProxy version 7.0.0 through 7.0.7 FortiProxy all versions 2.0, 1.2, 1.1, 1.0
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-22-297 https://www.fortiguard.com/psirt/FG-IR-23-069 https://www.fortiguard.com/psirt/FG-IR-22-452 https://www.fortiguard.com/psirt/FG-IR-23-013 https://www.fortiguard.com/psirt/FG-IR-22-464 https://www.fortiguard.com/psirt/FG-IR-22-456 https://www.fortiguard.com/psirt/FG-IR-22-520 https://www.fortiguard.com/psirt/FG-IR-22-407 https://www.fortiguard.com/psirt/FG-IR-22-475	

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.