Advisory Alert

Alert Number: AAA20210819 **Date:** August 19, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	OS Command Injection Vulnerability
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	Fortinet
Severity	**Critical**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2021-22123)
Description	Fortinet has released security updates addressing OS command injection vulnerability that exists in their products. CVE-2021-22123 – Successful exploitation of this flow may allow a remote authenticated attacker to execute arbitrary commands on the system via the SAML server configuration page. Fortinet highly recommends to apply necessary security fixes to avoid issues.
Affected Products	FortiWeb version 6.4.0 and below. FortiWeb version 6.3.14 and below. FortiWeb version 6.2.4 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-116

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1561, CVE-2021-34734)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-1561 - Successful exploitation of this vulnerability in spam quarantine feature of Cisco Secure Email and Web Manager could allow an authenticated remote attacker to gain unauthorized access and modify the spam quarantine settings of another user. CVE-2021-34734 - This vulnerability is due to improper management of memory resources and successful exploitation of this flaw could allow an unauthenticated adjacent attacker to cause a denial of service (DoS) condition. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Secure Email and Web Manager releases earlier than Release 14.1 Cisco Video Surveillance 7000 Series IP Cameras firmware Release 2.12.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-spam-jPxUXMk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-dos-OFP7j9j

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.