Advisory Alert

Alert Number: AAA20210602 **Date:** June 2, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	SAML Implementation Vulnerability
Fortinet	**High**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	SAML Implementation Vulnerability (CVE-2021-28091)
Description	Lasso disclosed a security vulnerability in the Lasso Security Assertion Markup Language Single Sign-On library. This risk may allow a verified attacker to pretend to be another authorized user when interacting with an application.
Affected Products	Cisco Adaptive Security Appliance (ASA) Software Cisco Content Security Management Appliance (SMA) Cisco Email Security Appliance (ESA) Cisco Web Security Appliance (WSA) Cisco Firepower Threat Defense (FTD) Software ASA Software FXOS Software FTD Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lasso-saml-jun2021-DOXNRLkD

Affected Product	Fortinet
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-13374, CVE-2021-24005, CVE-2021-26092, CVE-2021-24012, CVE-2021-22130, CVE-2018-13382, CVE-2018-13379, CVE-2021-26111, CVE-2021-26093, CVE-2021-22123, CVE-2021-22126, CVE-2018-13374)
Description	Fortinet has released security patch updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could cause Escalation of Privilege, denial of service, Remote Code Execution, Information Disclosure, Cross-site Scripting (XSS), Impersonation, Improper Access Control, Execute unauthorized code or commands effects on the systems.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-18-157 https://www.fortiguard.com/psirt/FG-IR-20-049 https://www.fortiguard.com/psirt/FG-IR-20-199 https://www.fortiguard.com/psirt/FG-IR-21-018 https://www.fortiguard.com/psirt/FG-IR-21-006 https://www.fortiguard.com/psirt/FG-IR-20-231 https://www.fortiguard.com/psirt/FG-IR-20-233 https://www.fortiguard.com/psirt/FG-IR-21-026 https://www.fortiguard.com/psirt/FG-IR-21-002 https://www.fortiguard.com/psirt/FG-IR-20-120 https://www.fortiguard.com/psirt/FG-IR-20-147 https://www.fortiguard.com/psirt/FG-IR-18-157

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.