Advisory Alert

Alert Number: AAA20220504 **Date:** May 4, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities
Fortinet	**High**	Multiple Vulnerabilities
OpenSSL	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20759, CVE-2022-20795)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist with Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. • **CVE-2022-20795**: A vulnerability in Cisco ASA Software and Cisco FTD Software's web services interface for remote access VPN features could allow an authenticated but unprivileged remote attacker to escalate privileges. • **CVE-2022-20795**: A vulnerability in Cisco ASA Software and Cisco FTD Software's implementation of the Datagram TLS (DTLS) protocol could allow an unauthenticated, remote attacker to cause high CPU utilization and cause a denial of service (DoS) condition. It is highly recommended to apply the necessary fixes provided on the official Cisco website at the earliest to avoid these security issues.
Affected Products	Cisco Adaptive Security Appliance Software Cisco Firepower Threat Defense Software Web Services Interface
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vpndtls-dos-TunzLEV

Affected Product	**Fortinet**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-43066, CVE-2021-41020, CVE-2022-26116, CVE-2021-43206, CVE-2021-41032, CVE-2022-22306, CVE-2021-43081, CVE-2022-23443, CVE-2021-37706)
Description	Fortinet has released Security Updates addressing multiple vulnerabilities that exist with Fortinet products. These vulnerabilities allow Privilege Escalation, SQL Injection, Information Disclosure, Improper Access Control, XSS, or launch Man-In-The-Middle attacks on the affected systems. It is highly recommended to apply the necessary fixes provided on the official Fortinet website at the earliest to avoid these security issues.
Affected Products	FortiClient FortiIsolator FortiNAC FortiOS FortiProxy FortiSOAR FortiFone
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt?date=05-2022

Affected Product	**OpenSSL**
Severity	**Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1292, CVE-2022-1343, CVE-2022-1434, CVE-2022-1473)
Description	OpenSSL has released a Security Advisory to address two moderate and two low severity fixes that exist with multiple OpenSSL versions. These vulnerabilities allow Command injection, incorrectly verifying the response signing certificate, Incorrect MAC key used in the RC4-MD5 cipher suite, and Resource leakage when decoding certificates and keys on the affected systems. It is highly recommended to apply the necessary fixes provided on the official OpenSSL website at the earliest to avoid these security issues.
Affected Products	OpenSSL
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20220503.txt

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.