Advisory Alert

Alert Number: AAA20220707 **Date:** July 7, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**,	Multiple Vulnerabilities
OpenSSL	**High**	Heap memory corruption vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20812, CVE-2022-20813)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS). **CVE-2022-20812** – A vulnerability exists because of the insufficient input validation of user-supplied command arguments. A remote attacker with Administrator read-write privileges can submit the crafted input to the affected command leading to arbitrary file overwrite on the underlying operating system as the root user. **CVE-2022-20813** – A null byte poisoning vulnerability that exists because of the improper certificate validation. An attacker can exploit this vulnerability by using a man in the middle attack to monitor the traffic and using a crafted certificate, the attacker can intercept traffic in clear text or alter the contents of the traffic. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Expressway Series and Cisco TelePresence VCS Release V 14.0 and earlier.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20791,CVE-2022-20808, CVE-2022-20752, CVE-2022-20862, CVE-2022-20859, CVE-2022-20768, CVE-2022-20815, CVE-2022-20800, CVE-2022-20791)
Description	Cisco has released a patch update addressing multiple flaws that exist their products. If exploited these vulnerabilities can lead to denial-of-service conditions, timing attacks, Arbitrary file reads, Unwanted access control using administrative privileges, Software information disclosure and Cross site scripting. Cisco highly recommends to apply necessary fixes to avoid issues.
Affected Products	Cisco SSM On-Prem Release V8 and earlier. Cisco Unified CM and Cisco Unified CM SME Release V14.0 and earlier Cisco Unity Connection Release 14.0 and earlier Cisco TelePresence CE Software Release V10 and earlier Cisco Unified CM IM&P Release version 14.0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-privesc-tP6uNZOS https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-timing-JVbHECOK https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-file-read-qgjhEc3A https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-access-dMKvV2DY https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-infodisc-YOTz9Ct7 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-ksKd5yfA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-RgH7MpKA

Affected Product	**FortiGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-26120, CVE-2022-27483, CVE-2021-43072, CVE-2021-41031, CVE-2022-30302, CVE-2022-29057, CVE-2022-26118, CVE-2022-26117, CVE-2021-44170, CVE-2022-23438, CVE-2021-42755)
Description	FortiGuard has released security updates to address multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could cause SQL injection, Arbitrary code execution, buffer overflow, privilege escalation, path traversal, reflected cross site scripting attack (XSS), denial of service. FortiGuard highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiADC version 7.0.0 through 7.0.1 FortiADC version 6.2.0 through 6.2.2 FortiADC version 6.1.0 through 6.1.6 FortiADC version 6.0.0 through 6.0.4 FortiADC version 5.4.0 through 5.4.5 FortiADC version 5.3.0 through 5.3.7 FortiADC version 5.2.0 through 5.2.8 FortiADC version 5.1.0 through 5.1.7 FortiADC version 5.0.0 through 5.0.4 FortiManager version 7.0.0 through 7.0.3 FortiManager version 6.4.0 through 6.4.7 FortiManager version 6.2.0 through 6.2.9 FortiManager version 6.0.0 through 6.0.11 FortiAnalyzer version 7.0.0 through 7.0.3 FortiAnalyzer version 6.4.0 through 6.4.7 FortiAnalyzer version 6.2.0 through 6.2.9 FortiAnalyzer version 6.0.0 through 6.0.11 FortiManager version 5.6.0 through 5.6.11 FortiManager version 7.0.0 through 7.0.2 FortiAnalyzer version 5.6.0 through 5.6.11 FortiAnalyzer version 7.0.0 through 7.0.2 FortiOS version 6.0.0 through 6.0.14 FortiOS version 6.2.0 through 6.2.10 FortiOS version 6.4.0 through 6.4.8 FortiOS version 7.0.0 through 7.0.5 FortiProxy version 1.0.0 through 1.0.7 FortiProxy version 1.1.0 through 1.1.6 FortiProxy version 1.2.0 through 1.2.13 FortiProxy version 2.0.0 through 2.0.8 FortiProxy version 7.0.0 through 7.0.3 FortiClientWindows version 7.0.0 through 7.0.2 FortiClientWindows version 6.4.0 through 6.4.6 FortiClientWindows version 6.2.0 through 6.2.9 FortiDeceptor version 1.0.0 through 1.0.1 FortiDeceptor version 1.1.0 FortiDeceptor version 2.0.0 FortiDeceptor version 2.1.0 FortiDeceptor version 3.0.0 through 3.0.2 FortiDeceptor version 3.1.0 through 3.1.1 FortiDeceptor version 3.2.0 through 3.2.2 FortiDeceptor version 3.3.0 through 3.3.2 FortiDeceptor version 4.0.0 through 4.0.1 FortiEDR Central Manager version 4.0.0 FortiEDR Central Manager version 5.0.0 through 5.0.3 Patch 6 FortiEDR Central Manager version 5.1.0 FortiNAC version 8.3.7 FortiNAC version 8.5.0 through 8.5.2 FortiNAC version 8.5.4 FortiNAC version 8.6.0 FortiNAC version 8.6.2 through 8.6.5 FortiNAC version 8.7.0 through 8.7.6 FortiNAC version 8.8.0 through 8.8.11 FortiNAC version 9.1.0 through 9.1.5 FortiNAC version 9.2.0 through 9.2.3 FortiProxy version 2.0.0 through 2.0.7 FortiOS version 7.0.0 through 7.0.2 FortiOS version 6.4.0 through 6.4.9 FortiOS version 7.0.2 and below. FortiOS version 6.4.8 and below. FortiOS version 6.2.x. FortiOS version 6.0.x. FortiProxy version 7.0.0. Fortiproxy version 2.0.6 and below. FortiProxy version 1.2.x. FortiProxy version 1.1.x. FortiProxy version 1.0.x. FortiSwitch version 7.0.2 and below. FortiSwitch version 6.4.9 and below. FortiSwitch version 6.2.x. FortiSwitch version 6.0.x. FortiRecorder version 6.4.2 and below. FortiRecorder version 6.0.10 and below. FortiVoiceEnterprise version 6.4.3 and below. FortiVoiceEnterprise version 6.0.10 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-051 https://www.fortiguard.com/psirt/FG-IR-22-049 https://www.fortiguard.com/psirt/FG-IR-21-206 https://www.fortiguard.com/psirt/FG-IR-21-190 https://www.fortiguard.com/psirt/FG-IR-21-213 https://www.fortiguard.com/psirt/FG-IR-22-077 https://www.fortiguard.com/psirt/FG-IR-21-056 https://www.fortiguard.com/psirt/FG-IR-22-058 https://www.fortiguard.com/psirt/FG-IR-21-179 https://www.fortiguard.com/psirt/FG-IR-21-057 https://www.fortiguard.com/psirt/FG-IR-21-155

Affected Product	**OpenSSL**
Severity	**High**
Affected Vulnerability	Heap memory corruption vulnerability (CVE-2022-2274)
Description	Openssl has released a security update to address a heap memory corruption vulnerability that exist in their products. **CVE-2022-2274**- OpenSSL 3.0.4 contains a flaw in the RSA implementation for X86_64 CPUs that support the AVX512IFMA instructions. This issue causes an incorrect RSA implementation for 2048-bit private keys. As a result, heap memory corruption occurs during computation. As a consequence of this memory corruption an attacker may be able to trigger RCE on the machine performing the computation. OpenSSL highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	OpenSSL 1.1.1 OpenSSL 3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20220705.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.