Advisory Alert

Alert Number: AAA20210218 **Date:** February 18, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	High	Multiple Vulnerabilities
OpenSSL	Medium	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerabilities	Multiple Vulnerabilities (CVE-2021-1366, CVE-2021-1372)
Description	Cisco have released Security Updates which addresses multiple Vulnerabilities across several products. CVE-2021-1366 - A vulnerability in the IPC channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated local attacker to send a crafted IPC message to Any-Connect process to execute arbitrary code on the affected machine with System privileges. CVE-2021-1372 - A vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated local attacker with permissions to view system memory. Attacker can run a specially crafted program to read shared memory of the affected application and obtain usernames, meeting information, or authentication tokens.
Affected Products	Cisco AnyConnect Secure Mobility Client for Windows releases earlier than Release 4.9.05042 that have the VPN Posture (HostScan) Module installed. Cisco Webex Meetings Desktop App and Cisco Webex Productivity Tools releases earlier than re-leases 40.6 and 40.10 when they are running on a Microsoft Windows end-user system. Cisco Webex Meetings Server Desktop App and Cisco Webex Productivity Tools releases that are included with Cisco Webex Meeting Server releases earlier than Release 4.0MR3 SP4 when they are running on a Microsoft Windows end-user system.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Re-leased	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-hijac-JrcTOQMC https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wda-pt-msh-6LWOcZ5

Affected Product	OpenSSL
Severity	**Medium**
Affected Vulnerabilities	Multiple Vulnerabilities (CVE-2021-23841, CVE-2021-23840, CVE-2021-23839)
Description	OpenSSL have released Security Updates which addresses multiple Vulnerabilities across several products. CVE-2021-23841- The vulnerability exists due to a NULL pointer dereference error within the X509_issuer_and_serial_hash() function when parsing the issuer field in the X509 certificate. A remote attacker can supply a specially crafted certificate, trigger a NULL pointer dereference error and perform a denial of service attack. CVE-2021-23840- The vulnerability exists due to insufficient validation of user supplied input during EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate calls. A remote attacker can pass specially crafted input to the application and perform a denial of service attack. CVE-2021-23839 - The vulnerability exists due to a faulty implementation of the padding check when server is configured to support SSLv2 protocol. A remote attacker can perform a man in the middle attack and force the server to use less secure protocols.
Affected Products	OpenSSL versions 1.1.1i and below OpenSSL versions 1.0.2x and below OpenSSL 1.0.2 servers from version 1.0.2s to 1.0.2x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20210216.txt https://www.openssl.org/news/vulnerabilities.html#y2021

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.