Security Advisory 2021-028

High Vulnerabilities in Cisco Products

June 17, 2021 — v1.0

TLP:WHITE

History:

- *17/06/2021 — v1.0 – Initial publication*

Summary

On 16th of June 2021, Cisco released security updates to address several security flaws [1]. The list includes two significant vulnerabilities. The first one is affecting Cisco Email Security Appliance and Cisco Web Security Appliance and it could allow man-in-the-middle (MitM) attack. The second one is affecting Cisco AnyConnect Secure Mobility Client for Windows and it allows a local user to escalate privileges on the system.

Technical Details

Critical Vulnerabilities

CVE-2021-1566

A vulnerability in the Cisco Advanced Malware Protection (AMP) for Endpoints integration of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to intercept traffic between an affected device and the AMP servers. This vulnerability is due to improper certificate validation when an affected device establishes TLS connections. A man-in-the-middle attacker could exploit this vulnerability by sending a crafted TLS packet to an affected device. A successful exploit could allow the attacker to spoof a trusted host and then extract sensitive information or alter certain API requests [2].

CVE-2021-1567

A vulnerability in the DLL loading mechanism of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for DLL files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with SYSTEM privileges. To exploit this vulnerability, the attacker must have valid credentials on the Windows system [3].

Other Vulnerabilities

Additionally to the critical vulnerabilities mentioned above Cisco announced several others, most notably:

- Cisco Small Business 220 Series Smart Switches Vulnerabilities - SIR: High
- Cisco DNA Center Certificate Validation Vulnerability - SIR: High

Products Affected

For CVE-2021-1566, vulnerable software versions are[2]:

- Cisco AsyncOS for Web Security Appliances: before 11.8.3-021, 12.0.3-005, 12.5.1-043
- Cisco AsyncOS for Cisco Email Security Appliance: before 12.5.3-035, 13.0.0-030, 13.5.3-010

This CVE-2021-1567 vulnerability affects Cisco AnyConnect Secure Mobility Client for Windows releases earlier than Release 4.10.01075 if the VPN Posture (HostScan) Module is installed.[3]

Recommendations

Cisco has released software updates that address these critical vulnerabilities [1, 2, 3].

There are no workarounds that address the critical vulnerabilities.

CERT-EU recommends updating the vulnerable application as soon as possible.

References

[1] https://tools.cisco.com/security/center/publicationListing.x

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-cert-valin8L97RW

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-posdll-ff8j6dFv