BLACKSWAN CYBERSECURITY

THREAT ADVISORY

February 20, 2024

Akira Ransomware Exploiting Cisco ASA/FTD Bug (CVE-2020-3259)

SUMMARY

CISA added CVE-2020-3259 to the Known Exploited Vulnerabilities catalog for a now-patched vulnerability affecting Cisco ASA and FTD software. The high-severity information disclosure issue could allow attackers to retrieve memory contents from affected devices. The Akira ransomware group appears to be exploiting this vulnerability to compromise Cisco Anyconnect SSL VPN appliances.

RISK SCORING

CVE-ID	Score
CVE-2020-3259	7.5

TECHNICAL DETAILS

This is an information disclosure vulnerability found in the web services interface of Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) products. It allows a remote, unauthenticated attacker to extract potentially sensitive data from an affected device's memory, including credentials. Although Cisco patched the flaw in 2020, it gained attention recently when Truesec discovered evidence suggesting exploitation by the Akira ransomware group.

Truesec's analysis of a recent incident response engagement, where Akira ransomware was involved and Cisco Anyconnect SSL VPN was the entry point, revealed that at least six compromised devices were running different versions of the vulnerable software.

AFFECTED PRODUCTS

Cisco Adaptive Security Appliance (ASA):

- Cisco ASA 9.x prior to release 9.51
- Cisco ASA 9.6 prior to release 9.6.4.41
- Cisco ASA 9.7 prior to release 9.71
- Cisco ASA 9.8 prior to release 9.8.4.20
- Cisco ASA 9.9 prior to release 9.9.2.67
- Cisco ASA 9.10 prior to release 9.10.1.40
- Cisco ASA 9.12 prior to release 9.12.3.9
- Cisco ASA 9.13 prior to release 9.13.1.10

Cisco Firepower Threat Defense (FTD):

- Cisco FTD 6,x prior to release 6.2.31
- Cisco FTD 6.2.3 prior to release 6.2.3.16
- Cisco FTD 6.3.0 prior to release 6.3.0.6
- Cisco FTD 6.4.0 prior to release 6.4.0.9
- Cisco FTD 6.5.0 prior to release 6.5.0.5

SOLUTION

Update Cisco Adaptive Security Appliance (ASA) to the respective release, as follows:

- Cisco ASA release 9.51
- Cisco ASA release 9.6.4.41
- Cisco ASA release 9.71
- Cisco ASA release 9.8.4.20
- Cisco ASA release 9.9.2.67
- Cisco ASA release 9.10.1.40
- Cisco ASA release 9.12.3.9
- Cisco ASA release 9.13.1.10

Updated Cisco Firepower Threat Defense (FTD) to the respective release, as follows:

- Cisco FTD release 6.2.31
- Cisco FTD release 6.2.3.16
- Cisco FTD release 6.3.0.6
- Cisco FTD release 6.4.0.9
- Cisco FTD release 6.5.0.5

MITIGATIONS

- Upgrade to the latest available version for ASA / FTD.
- For devices that are managed using Cisco Firepower Management Center (FMC), use the FMC interface to install the upgrade. After installation is complete, reapply the access control policy.
- For devices that are managed using Cisco Firepower Device Manager (FDM), use the FDM interface to install the upgrade. After installation is complete, reapply the access control policy.
- Implement MFA on all accounts and services where it is possible, especially for Client VPN connections.
- Force a password change, especially if there are accounts in the environment that were not changed after the version upgrade.
- Change secret and pre-shared keys in device configurations if not changed after the version upgrade.

REFERENCES

- https://www.securityweek.com/cisa-urges-patching-of-cisco-asa-flaw-exploited-in-ransomware-attacks/
- https://securityaffairs.com/159244/cyber-crime/cisa-cisco-cve-2020-3259-akira-ransomware.html
- https://appcheck-ng.com/cve-2020-3259/
- https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259