ultraviolet

CONFIDENTIAL

THREAT REPORT:

Akira Ransomware Threat Actors Observed Targeting Cisco ASA SSL VPNs with Credential Stuffing Attacks

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
8/28/2023

Doc ID: ECORP_SUM_07032023_v1.1

Contents

1 Executive Summary

Threat actors using Akira ransomware are stuffing leaked and purchased credentials into the Cisco Adaptive Security Appliance (ASA) SSL VPN service to gain initial access to networks. Researchers have observed successful authentication attempts at several organizations who use Cisco's ASA VPN service without MFA enabled. Targeted organizations with Multi-Factor Authentication enabled have seen authentication attempts denied once MFA was not verified by the associated user. Organizations using Cisco's ASA VPN service are advised to rotate passwords regularly and enable MFA where possible.

2 Technical Analysis

Cisco's Product Security Incident Response Team (PSIRT) posted on their website about attackers using Akira ransomware to automatically target Cisco VPNs to brute force login attempts. Through a mixture of brute force and credential stuffing, threat actors were able to breach at least eleven (11) customers during the second quarter of this year.

After successful initial access, threat actors were observed using AnyDesk's remote desktop service to harvest credentials by exploiting the Local Security Authority Subsystem Service (LSASS) to dump NTDS.DIT files from the network's Active Directory service or from the local host's process memory. Equipped with network credentials, threat actors moved laterally to hosts with strategic value and executed LockBit or Akira ransomware attacks.

While most successful unauthorized login attempts were associated with organizations with no MFA enabled, some activity has been noted where threat actors attempted to use known vulnerabilities in MFA. It is important to not just have MFA enabled but to ensure the service is up to date and all known vulnerabilities have been patched by administrators.

(443) 351-7630 | info@uvcyber.com

3 What UltraViolet Cyber is Doing

- Regularly updating our IOC & TTP databases to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- If your organization uses Cisco ASA for VPN, please ensure you have MFA enabled for all VPN users
- Practice regular password rotation within your organization and ensure passwords are not re-used after each rotation
- Disable default usernames and passwords to help block successful brute force login attempts
- Enable logging on all VPNs to aid with monitoring, detection and remediation efforts

5 References

Gatlan, S. Hacking campaign bruteforces Cisco VPNs to breach networks. Retrieved September 1, 2023, from https://www.bleepingcomputer.com/news/security/hacking-campaign-bruteforces-cisco-vpns-to-breach-networks/

Santos, O. Akira Ransomware Targeting VPNs without Multi-Factor Authentication. Retrieved September 1, 2023, from https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication

Starks, T., Beek, C., Knapp, R., Dayton, Z., & Condon, C. Under Siege: Rapid7-Observed Exploitation of Cisco ASA SSL VPNs. Retrieved September 1, 2023, from https://www.rapid7.com/blog/post/2023/08/29/under-siege-rapid7-observed-exploitation-of-cisco-asa-ssl-vpns/