Under Siege: Rapid7-Observed Exploitation of Cisco ASA SSL VPNs | Rapid7 Blog

By Rapid7

Published: 2023-08-29 · Archived: 2026-04-05 13:36:38 UTC

Tyler Starks, Christiaan Beek, Robert Knapp, Zach Dayton, and Caitlin Condon contributed to this blog.

Rapid7's managed detection and response (MDR) teams have observed increased threat activity targeting Cisco ASA SSL VPN appliances (physical and virtual) dating back to at least March 2023. In some cases, adversaries have conducted credential stuffing attacks that leveraged weak or default passwords; in others, the activity we've observed appears to be the result of targeted brute-force attacks on ASA appliances where multi-factor authentication (MFA) was either not enabled or was not enforced for all users (i.e., via MFA bypass groups). Several incidents our managed services teams have responded to ended in ransomware deployment by the Akira and LockBit groups.

There is no clear pattern among target organizations or verticals. Victim organizations varied in size and spanned healthcare, professional services, manufacturing, and oil and gas, along with other verticals. We have included indicators of compromise (IOCs) and attacker behavior observations in this blog, along with practical recommendations to help organizations strengthen their security posture against future attacks. **Note:** Rapid7 has not observed any bypasses or evasion of correctly configured MFA.

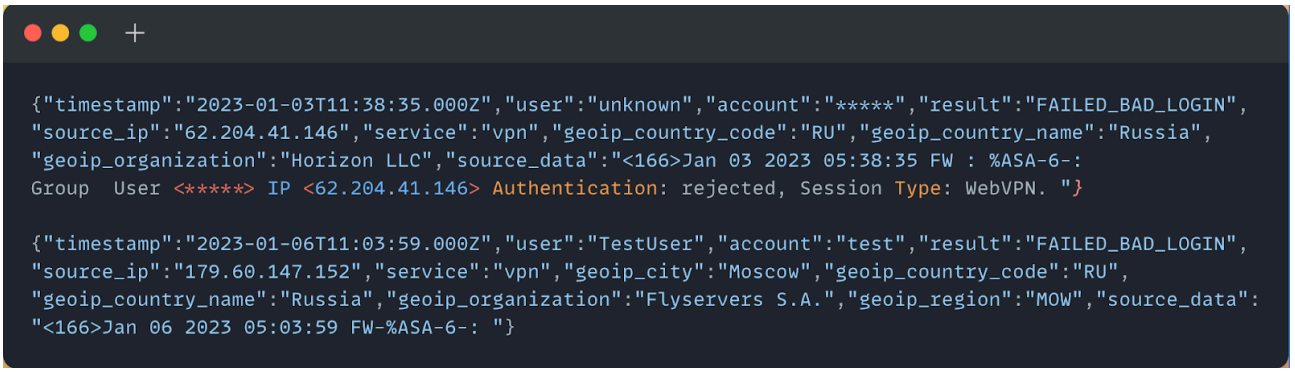
Rapid7 has been actively working with Cisco over the course of our investigations. On August 24, Cisco's Product Security Incident Response Team (PSIRT) published a blog outlining attack tactics they have observed, many of which overlap with Rapid7's observations. We thank Cisco for their collaboration and willingness to share information in service of protecting users.

Observed attacker behavior

Rapid7 identified at least 11 customers who experienced Cisco ASA-related intrusions between March 30 and August 24, 2023. Our team traced the malicious activity back to an ASA appliance servicing SSL VPNs for remote users. ASA appliance patches varied across compromised appliances — Rapid7 did not identify any particular version that was unusually susceptible to exploitation.

In our analysis of these intrusions, Rapid7 identified multiple areas of overlap among observed IOCs. The Windows clientname WIN-R84DEUE96RB was often associated with threat actor infrastructure, along with the IP addresses 176.124.201[.]200 and 162.35.92[.]242. We also saw overlap in accounts used to authenticate into internal systems, including the use of accounts TEST, CISCO, SCANUSER, and PRINTER. User domain accounts were also used to successfully authenticate to internal assets — in several cases, attackers successfully authenticated on the first try, which may indicate that the victim accounts were using weak or default credentials.

The below image is an anonymized log entry where an attacker attempts a (failed) login to the Cisco ASA SSL VPN service. In our analysis of log files across different incident response cases, we frequently observed failed login attempts occurring within milliseconds of one another, which points at automated attacks.



In most of the incidents we investigated, threat actors attempted to log into ASA appliances with a common set of usernames, including:

- admin
- adminadmin
- backupadmin
- kali
- cisco
- guest
- accounting
- developer
- ftp user
- training
- test
- printer
- echo
- security
- inspector
- test test
- snmp

The above is a fairly standard list of accounts that may point at use of a brute forcing tool. In some cases, the usernames in login attempts belonged to actual domain users. While we have no specific evidence of leaked victim credentials, we are aware that it's possible to attempt to brute force a Cisco ASA service with the path +CSCOE+/logon.htm. VPN group names are also visible in the source code of the VPN endpoint login page and can be easily extracted, which can aid brute forcing attacks.

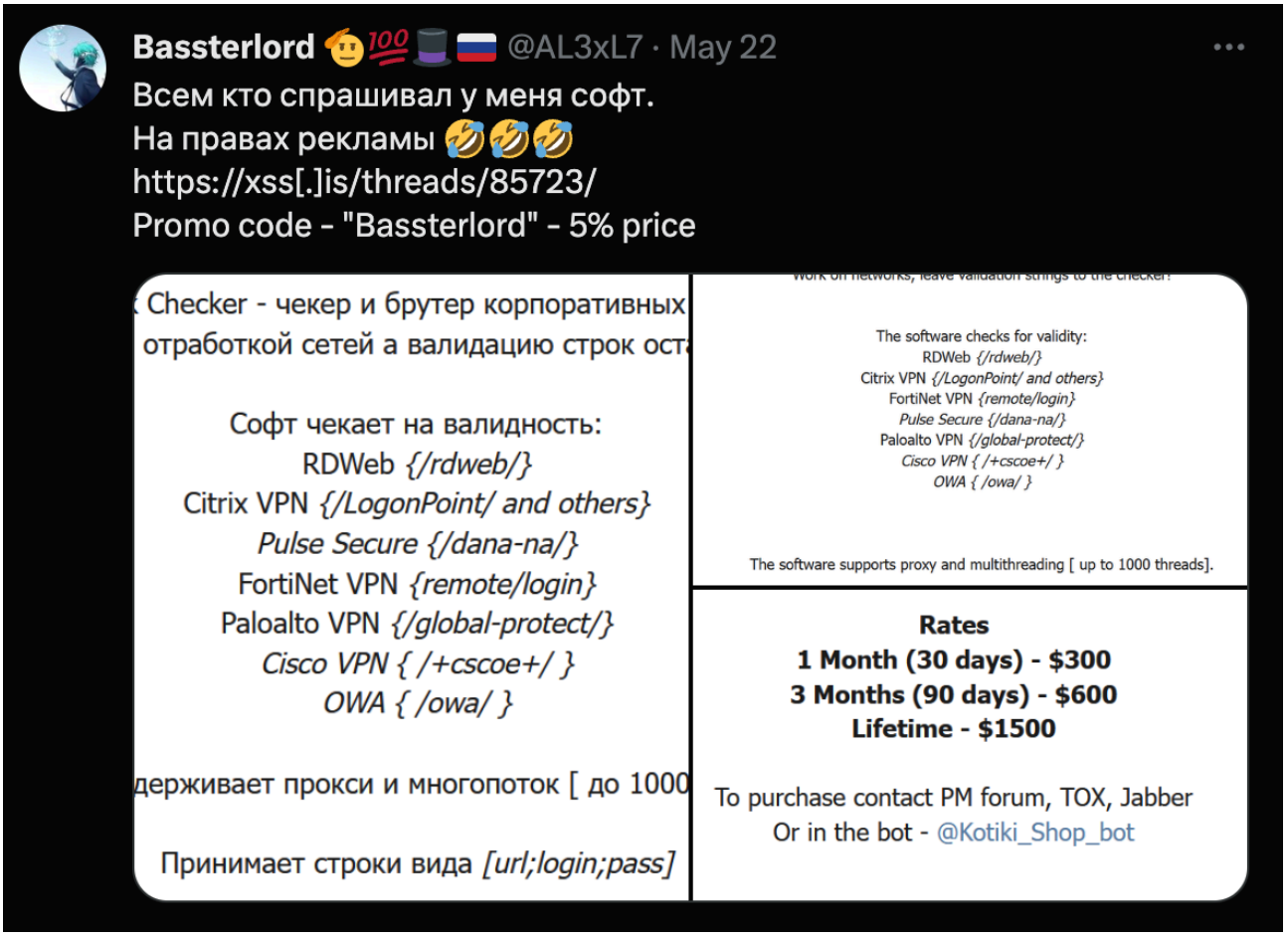
Upon successful authentication to internal assets, threat actors deployed set.bat. Execution of set.bat resulted in the installation and execution of the remote desktop application AnyDesk, with a set password of greenday#@!. In some cases, nd.exe was executed on systems to dump NTDS.DIT, as well as the SAM and SYSTEM hives, which may have given the adversary access to additional domain user credentials. The threat actors performed further

lateral movement and binary executions across other systems within target environments to increase the scope of compromise. As mentioned previously, several of the intrusions culminated in the deployment and execution of Akira or LockBit-related ransomware binaries.

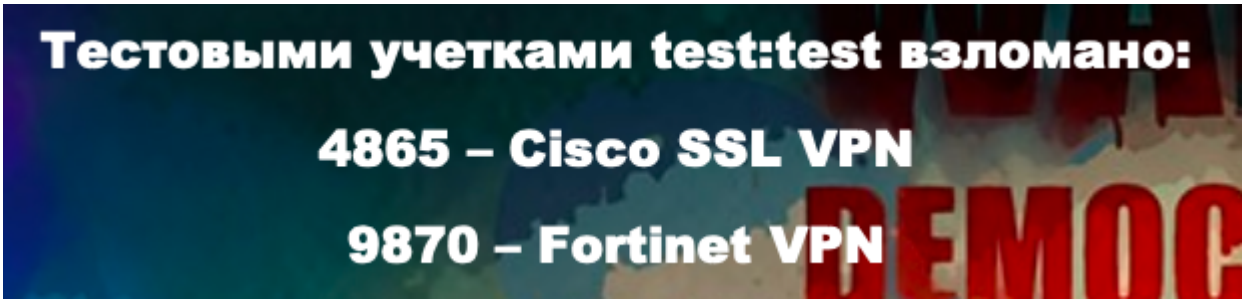
Dark web activity

In parallel with incident response investigations into ASA-based intrusions, Rapid7 threat intelligence teams have been monitoring underground forums and Telegram channels for threat actor discussion about these types of attacks. In February 2023, a well-known initial access broker called “Bassterlord” was observed in XSS forums selling a guide on breaking into corporate networks. The guide, which included chapters on SSL VPN brute forcing, was being sold for $10,000 USD.

When several other forums started leaking information from the guide, Bassterlord posted on Twitter about shifting to a content rental model rather than selling the guide wholesale:



Rapid7 obtained a leaked copy of the manual and analyzed its content. Notably, the author claimed they had compromised 4,865 Cisco SSL VPN services and 9,870 Fortinet VPN services with the username/password combination test:test. It’s possible that, given the timing of the dark web discussion and the increased threat activity we observed, the manual’s instruction contributed to the uptick in brute force attacks targeting Cisco ASA VPNs.



Indicators of compromise

Rapid7 identified the following IP addresses associated with source authentication events to compromised internal assets, as well as outbound connections from AnyDesk:

- 161.35.92.242
- 173.208.205.10
- 185.157.162.21
- 185.193.64.226
- 149.93.239.176
- 158.255.215.236
- 95.181.150.173
- 94.232.44.118
- 194.28.112.157
- 5.61.43.231
- 5.183.253.129
- 45.80.107.220
- 193.233.230.161
- 149.57.12.131
- 149.57.15.181
- 193.233.228.183
- 45.66.209.122
- 95.181.148.101
- 193.233.228.86
- 176.124.201.200
- 162.35.92.242
- 144.217.86.109

Other IP addresses that were observed conducting brute force attempts:

- 31.184.236.63
- 31.184.236.71
- 31.184.236.79
- 194.28.112.149
- 62.233.50.19
- 194.28.112.156

- 45.227.255.51
- 185.92.72.135
- 80.66.66.175
- 62.233.50.11
- 62.233.50.13
- 194.28.115.124
- 62.233.50.81
- 152.89.196.185
- 91.240.118.9
- 185.81.68.45
- 152.89.196.186
- 185.81.68.46
- 185.81.68.74
- 62.233.50.25
- 62.233.50.17
- 62.233.50.23
- 62.233.50.101
- 62.233.50.102
- 62.233.50.95
- 62.233.50.103
- 92.255.57.202
- 91.240.118.5
- 91.240.118.8
- 91.240.118.7
- 91.240.118.4
- 161.35.92.242
- 45.227.252.237
- 147.78.47.245
- 46.161.27.123
- 94.232.43.143
- 94.232.43.250
- 80.66.76.18
- 94.232.42.109
- 179.60.147.152
- 185.81.68.197
- 185.81.68.75

Many of the IP addresses above were hosted by the following providers:

- Chang Way Technologies Co. Limited
- Flyservers S.A.
- Xhost Internet Solutions Lp
- NFOrce Entertainment B.V.

- VDSina Hosting

Log-based indicators:

- Login attempts with invalid username and password combinations (%ASA-6-113015)
- RAVPN session creation (attempts) for unexpected profiles/TGs (%ASA-4-113019, %ASA-4-722041, %ASA-7-734003)

Mitigation guidance

As Rapid7's mid-year threat review noted, **nearly 40% of all incidents** our managed services teams responded to in the first half of 2023 stemmed from lack of MFA on VPN or virtual desktop infrastructure. These incidents reinforce that use of weak or default credentials remains common, and that credentials in general are often not protected as a result of lax MFA enforcement in corporate networks.

To mitigate the risk of the attacker behavior outlined in this blog, organizations should:

- Ensure default accounts have been disabled or passwords have been reset from the default.
- Ensure MFA is enforced across all VPN users, limiting exceptions to this policy as much as possible.
- Enable logging on VPNs: Cisco has information on doing this for ASA specifically here, along with guidance on collecting forensic evidence from ASA devices here.
- Monitor VPN logs for authentication attempts occurring outside expected locations of employees.
- Monitor VPN logs for failed authentications, looking for brute forcing and password spraying patterns.
- As a best practice, keep current on patches for security issues in VPNs, virtual desktop infrastructure, and other gateway devices.

Rapid7 is monitoring MDR customers for anomalous authentication events and signs of brute forcing and password spraying. For InsightIDR and MDR customers, the following non-exhaustive list of detection rules are deployed and alerting on activity related to the attack patterns in this blog:

- Attacker Technique - NTDS File Access
- Attacker Tool - Impacket Lateral Movement
- Process Spawned By SoftPerfect Network Scanner
- Execution From Root of ProgramData

Various sources have recently published pieces noting that ransomware groups appear to be targeting Cisco VPNs to gain access to corporate networks. Rapid7 strongly recommends reviewing the IOCs and related information in this blog and in Cisco's PSIRT blog and taking action to strengthen security posture for VPN implementations.

Updates

On September 6, Cisco published an advisory on CVE-2023-20269, an unauthorized access vulnerability affecting ASA and Firepower Threat Defense remote access VPNs. According to the advisory, CVE-2023-20269 arises from improper separation of authentication, authorization, and accounting (AAA) between the remote access VPN feature and the HTTPS management and site-to-site VPN features. Successful exploitation could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and

password combinations or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user.

CVE-2023-20269 is being exploited in the wild and is related to some of the behavior Rapid7 has observed and outlined in this blog. A software update for Cisco ASA and FTD is pending. In the meantime, Cisco has workarounds and additional information in their advisory.

Download Rapid7's 2023 Mid-Year Threat Report ▶
