TLP:CLEAR

CYBER SECURITY ADVISORY

April 24, 2024

Co-Authored by:

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Cyber Activity Impacting CISCO ASA VPNs

ISBN 978-0-660-71567-4
CAT D96-111/2024E-PDF

TLP:CLEAR

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Foreword

THIS CYBER SECURITY ADVISORY IS INTENDED FOR IT PROFESSIONALS AND MANAGERS WITHIN GOVERNMENT AND ALL SECTORS.

Effective Date

This publication takes effect on April 24, 2024

Revision History

Revision	Amendments	Date
1	First release.	April 24, 2024

1 Background

Since early 2024, the Canadian Centre for Cyber Security (Cyber Centre), Australian Signals Directorate's Australian Cyber Security Centre and The UK's National Cyber Security Centre (NCSC) have been evaluating ongoing malicious cyber activity targeting virtual private network (VPN) services used by government and critical national infrastructure networks globally. The capabilities are indicative of espionage conducted by a well-resourced and sophisticated state-sponsored actor. There are no indicators suggesting that this threat activity is currently being used to preposition for disruptive or destructive computer network attack.

The sophistication demonstrated by the threat actors' use of multiple layers of novel techniques and the concurrent operations against multiple targets around the world is cause for concern to the authoring agencies. Since VPN services are essential components of computer network security, vulnerabilities in such services are particularly consequential and a public disclosure of critical vulnerabilities can enable their use by a wide variety of threat actors. We emphasize the need to patch devices quickly and to have a comprehensive defense in depth strategy such as applying the recommendations in this Security Advisory.

The authoring agencies can report the affected products are predominantly CISCO ASA devices, series ASA55xx and running firmware ASA versions 9.12 and 9.14. These affected products have been compromised by malicious actors who successfully established unauthorized access through WebVPN sessions, commonly associated with Clientless SSLVPN services.

The authoring agencies performed analysis that showed malicious actors abusing WebVPN by transmitting malicious payloads resulting in unauthorized remote code execution on Cisco devices. These commands include, but are not limited to, the configuration of packet capture sessions on the devices to collect and exfiltrate data. The authoring agencies continue to work closely with the vendor to better understand this novel method of compromise.

2 Artifacts

Detailed below are two samples of observed activity outlining communications between the malicious actors and the targeted devices. These samples are commands that directed the devices to perform specific actions which resulted in the exfiltration of device configurations, configuration of network captures, and data exfiltration.

The authoring agencies have identified these commands as two malware components related to the malicious activity targeting Cisco ASA devices as:

- LINE RUNNER - a persistent webshell enabling malicious actors to upload and execute arbitrary Lua scripts.
- LINE DANCER - an in-memory implant enabling malicious actors to upload and execute arbitrary shellcode payloads.

The authoring agencies believe these components are related due to the transient use of shared actor-created resources on an impacted device.

It is suspected that LINE RUNNER may be present on a compromised device even if LINE DANCER is not (e.g. as a persistent backdoor, or where an impacted ASA has not yet received full operational attention from the malicious actors). As such, any previous detection work for LINE DANCER with negative findings does not imply that LINE RUNNER is not present.

2.1 HTTP Requests (LINE RUNNER)

LINE RUNNER is a persistent Lua-based webshell targeting the Cisco Adaptive Security Appliance (ASA) WebVPN device customization functionality. LINE RUNNER implements multiple defense evasion techniques to avoid detection and prevent recovery via forensics. LINE RUNNER offers the ability to run arbitrary Lua code sent via HTTP GET requests to legitimate Cisco ASA WebVPN / AnyConnect URIs. E.g.:

```
GET /+CSCOE+/portal.css?<aaa>=<token>&<bbb>=<lua_script>
```

Where:

- <aaa> is a randomized query parameter key name.
- <token> is a randomized value, checked by the webshell (i.e., auth)
- <bbb> is a randomized query parameter key name.
- <lua_script> is the URL Encoded Lua commands to execute.

The use of randomized query parameters prevents mass scanning of potentially impacted ASAs. It is assumed the values in the GET requests are victim specific, but this is yet to be confirmed.

2.2 HTTP Request and Response (LINE DANCER)

LINE DANCER is a persistent Lua-based shellcode loader, which is a component of a larger framework. This shellcode loader would process malicious payloads that execute system commands. LINE DANCER offers the ability to run shellcode payloads -- these are base64-decoded and only run when prepended by a fixed 32-byte value, which differs between victims. Provided below is an example of HTTP POST requests to Cisco ASA WebVPN / AnyConnect URIs. E.g.:

```
POST /CSCOSSLC/config-auth HTTP/1.1

…

<host-scan-reply>[base64-encoded payloads]</host-scan-reply>
```

To further aid in detection and remediation options for organizations, the authoring agencies are providing additional examples of activity undertaken by the malicious actors:

- The malicious actors generated text versions of the device's configuration file so that it could be exfiltrated through web requests.
- The malicious actors were able to control the enabling and disabling of the devices syslog service to obfuscate additional commands.
- The malicious actors were able to modify the authentication, authorization and accounting (AAA) configuration so that specific actor-controlled devices matching a particular identification could be provided access within the impacted environment.

Cisco has assigned the following CVEs as being associated with LINE RUNNER [10] and LINE DANCER [11] activity:

CVE-2024-20353	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability
CVE-2024-20359	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability

Additional information on these vulnerabilities can be found by visiting the Cisco Security Advisories portal [7][8] and the Cisco Talos Blog. [9]

3 Indicators of Compromise

3.1 IP Addresses

The authoring agencies have observed the following malicious IP addresses targeting networks. The below can be considered high confidence indicators of malicious activity and organizations are reminded not to probe the provided IP addresses, but instead to check historical network logs, specifically for large volumes of data being transferred. Particular attention should be given if these IP addresses were observed through December 2023 to February 2024:

185.244.210[.]65	216.238.74[.]95
5.183.95[.]95	45.128.134[.]189
213.156.138[.]77	176.31.18[.]153
45.77.54[.]14	216.238.72[.]201
45.77.52[.]253	216.238.71[.]49
45.63.119[.]131	216.238.66[.]251
194.32.78[.]183	216.238.86[.]24
185.244.210[.]120	216.238.75[.]155
216.238.81[.]149	154.39.142[.]47
216.238.85[.]220	139.162.135[.]12

4 Recommended Actions

Cisco made the authoring agencies aware that recent firmware versions contained patches to aid in the mitigation of this activity. The patches updated firmware address techniques that had allowed malicious actors to gain persistence during the compromise. Organizations are encouraged to monitor future articles and firmware updates from Cisco and apply necessary patches when available.

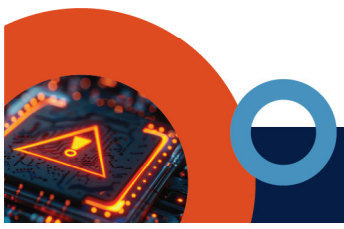
Patches are currently available for download from Cisco's website [5], which can be accessed via a valid Cisco account and active Cisco support contract for ASA devices. Organizations are encouraged to update to the latest patch versions, which would contain the relevant fixes associated with this activity and other updates available for the device. As of this publication the most recent versions available are:

- 9.16.4.57
- 9.18.4.22
- 9.20.2.10

4.1 Update instructions for supported devices

Cisco provided the following instructions on the update process.

- Visit Cisco's Software Download Centre https://software.cisco.com/download/home/
- Click on Browse All
- Choose Security > Firewalls.
- Depending on the desired hardware platform choose 3000 Series Industrial Security Appliances (ISA), Adaptive Security Appliances (ASA), or Next-Generation Firewalls (NGFW).
- Choose a specific product from the right pane of the product selector (depending on the exact hardware platform you may need to repeat this step).
- Choose Adaptive Security Appliance (ASA) Software.
- Navigate to All Release > Interim > 9 > 9.x.y Interim (example: 9.18.4 Interim). Note: Navigating to "Interim" within the steps listed above is important, otherwise you will not find the appropriate releases.



4.2 Update instructions for unsupported devices

For all unsupported devices that have entered End of Life (EoL), organizations are encouraged to contact Cisco to discuss alternative solutions. The authoring agencies wish to remind organizations of the importance of device lifecycle management. Using outdated software or hardware limits a manufacturer from providing security patches.

For further guidance, contact your support organization. If that is the Cisco TAC visit https://cisco.com/support/ or by phone at 800-553-2447 (US/Canada) to open a case with "**ARCANEDOOR**" as the reference code. International phone support numbers can be found on Cisco's website here: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

4.3 Heightened detection recommendation

The authoring agencies recommend the following actions for organizations to better protect themselves and to aid in the detection of malicious activity:

1. Upgrade devices running vulnerable firmware to a version that includes relevant fixes. Running the most recent firmware ensures that devices are best protected against newly discovered vulnerabilities.
2. If an upgrade path to the new firmware is not available, decommission the device or ensure that WebVPN services have been disabled.
3. Ensure proper hardware and software lifecycle management to benefit from vendor support and security updates.
4. As of September 30, 2019, Cisco has discontinued support for WebVPN [6]. If still in use, organizations are encouraged to plan on the migration of remote access connectivity to a supported technology.
5. Organizations are encouraged to review logs to filter for any unknown, unexpected, or unauthorized access or changes to devices. Organizations should also monitor for unexpected activity such as unexpected reboots, large transfers to unknown IP Addresses and gaps in logging, which may indicate the disabling of logging services.
6. Enable 'informational' logging on all Cisco ASA devices [1]
7. Ensure that off-device logging is sufficient to support historical analysis, particularly if the syslog severity logging is increased.
8. Validate with administrators if any of the alert codes below are observed to review for potential malicious activity.

ASA Code	Descriptions
ASA-4-106103	access-list acl_ID denied protocol for user username
ASA-4-109027	[aaa protocol] Unable to decipher response message
ASA-4-113019	Session disconnected.
ASA-4-315009	SSH: connection timed out
ASA-4-717037	Tunnel group search using certificate maps failed for peer certificate
ASA-4-722041	No IPv6 address available for SVC connection
ASA-4-768003	SSH: connection timed out
ASA-5-111001	Begin configuration: IP_address writing to device
ASA-5-111003	IP_address Erase configuration
ASA-5-111008	User user executed the command string
ASA-5-212009	Configuration request for SNMP group groupname failed.
ASA-5-718072	Becoming master of Load Balancing in context
ASA-5-734002	Connection terminated by the following DAP records
ASA-5-8300006	Cluster topology change detected. VPN session redistribution aborted
ASA-6-113015	AAA user authentication Rejected
ASA-7-734003	DAP: User name, Addr ipaddr: Session Attribute: attr name/value

4.4 Hardening Recommendations

The following hardening recommendations will impact the malicious actor's ability to conduct malicious activity based on observed tactics, techniques, and procedures (TTPs):

1. Disable or restrict internal unencrypted traffic through gateway devices, including Server Message Block (SMB) traffic. SMB 3.0 or higher can be configured to use encryption. Earlier versions of SMB should not be used.
2. Enable strong SNMPv3 access and deprecate SNMPv2.
3. Accounts and credentials used on edge devices and integrated into internal systems, such as Active Directory, could be exploited by malicious actors. These shared accounts should have the minimum necessary privileges to reduce a malicious actors ability to compromise other services. These accounts should be closely monitored to identify any deviations from expected behaviour.
4. Based on the observed TTPs, the authoring agencies recommend enforcing the use of Internet Protocol Security (IPsec) rather than Secure Socket Layer/Transport Layer Security (SSL/TLS) for VPN connectivity. Organizations should consider configuring all services to block public access to the SSL components of the ASA device. [2][3]
5. If Secure Socket Layer/Transport Layer Security (SSL/TLS) for VPN, or other external facing services such as Secure Shell (SSH) are required, organizations should use the latest secure protocols with recommended cipher suites and hardening recommendations provided by the Cyber Centre through ITSP.40.062. [4]
6. Where feasible, utilize Access Control Lists (ACLs) to block external access to the VPN device from known malicious IP addresses. ACLs can also be configured to only permit access from countries from which remote users are expected to connect from; a process known as "Geofencing".
7. Utilize threat detection techniques, centralized log collection, security information and event management and adequate alerting / reporting.

5 References

Number	Reference
1	Cisco Secure Firewall ASA Series Syslog Messages https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog/syslogs-sev-level.html
2	Selecting and Hardening Remote Access VPN Solutions https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
3	Device Security Guidance - Virtual Private Networks (VPNs) https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks
4	Guidance on securely configuring network protocols (ITSP.40.062) https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062
5	Cisco Software Download https://software.cisco.com/download/home/
6	Cisco End-of-Sale and End-of-Life Announcement for the Clientless SSL VPN (WebVPN) on Cisco IOS Software https://www.cisco.com/c/en/us/products/collateral/security/ios-sslvpn/eos-eol-notice-c51-731468.html
7	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2
8	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h
9	ArcaneDoor: New espionage-focused campaign targets perimeter network devices https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
10	NCSC Malware Tipper - LINE RUNNER https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-runner.pdf
11	NCSC Malware Tipper - LINE DANCER https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-dancer.pdf