TLP:CLEAR

BULLETIN DE CYBERSÉCURITÉ

Le 24 avril 2024

Corédigé par :

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Cyberactivité touchant les réseaux privés virtuels Cisco ASA

ISBN 978-0-660-71568-1
CAT D96-111/2024F-PDF

TLP:CLEAR

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

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Canada

Avant-propos

LE PRÉSENT BULLETIN DE CYBERSÉCURITÉ S'ADRESSE AUX GESTIONNAIRES AINSI QU'AUX PROFESSIONNELLES ET PROFESSIONNELS DES TI ŒUVRANT AU SEIN DU GOUVERNEMENT ET DE TOUS LES SECTEURS.

Date d'entrée en vigueur

La présente documentation entre en vigueur le 24 avril 2024.

Historique des révisions

Révision	Modifications	Date
1	Première version.	24 avril 2024

1 Context

Depuis le début de 2024, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité), l'Australian Cyber Security Centre (ACSC) de l'Australian Signals Directorate (ASD) et le National Cyber Security Centre du Royaume-Uni (NCSC-UK) ont procédé à l'évaluation d'une cyberactivité malveillante continue ciblant les services de réseau privé virtuel (RPV) utilisés sur les réseaux des gouvernements et des infrastructures nationales critiques à travers le monde. Les capacités sont révélatrices d'un espionnage pratiqué par une ou un auteur de menace parrainé par un État doté de moyens sophistiqués et de ressources considérables. Rien ne semble indiquer que cette activité de cybermenace soit actuellement utilisée dans le but de mettre en place une attaque perturbatrice ou destructive contre des réseaux informatiques.

Les organismes ayant rédigé la présente sont préoccupés par la sophistication des techniques multicouches innovantes qu'utilisent les auteures et auteurs de menace, ainsi que par les activités qui ont été menées concurremment contre plusieurs cibles à l'échelle mondiale. Comme les services RPV sont des composants essentiels de la sécurité des réseaux informatiques, les vulnérabilités liées à de tels services sont particulièrement substantielles et une divulgation publique de vulnérabilités critiques pourrait permettre à un large éventail d'auteures et auteurs de menace d'y avoir recours. Il convient de souligner la nécessité d'appliquer rapidement des correctifs aux dispositifs et de mettre en place une stratégie exhaustive de défense en profondeur, comme l'application des recommandations formulées dans le présent bulletin de sécurité.

Les organismes ayant rédigé la présente peuvent indiquer que les produits touchés sont principalement des appliances de sécurité adaptative (ASA) de Cisco de la série ASA55x et ceux exécutant les versions micrologicielles 9.12 et 9.14 de l'ASA. Les produits touchés ont été compromis par des auteures et auteurs de menace ayant réussi à établir un accès non autorisé par l'intermédiaire de sessions WebVPN, communément associées aux services de RPV SSL sans client.

Les organismes ayant rédigé la présente ont procédé à une analyse qui a révélé que des auteures et auteurs de menace abusaient de WebVPN en transmettant des charges de virus malveillantes dans le cadre d'une exécution non autorisée de code à distance sur des dispositifs Cisco. Ces commandes visaient notamment à configurer des sessions de capture de paquets sur des dispositifs en vue de collecter et d'exfiltrer les données. Les organismes ayant rédigé la présente continuent de travailler étroitement avec le fournisseur pour mieux comprendre cette nouvelle méthode de compromission.

2 Artéfacts

On trouve ci-dessous deux échantillons d'activités observées illustrant les communications entre les auteurs et auteurs de menace et les dispositifs ciblés. Il s'agit de commandes qui ordonnaient aux dispositifs d'effectuer des actions particulières, ce qui a mené à l'exfiltration des configurations du dispositif, à la configuration de captures du réseau et à l'exfiltration de données.

Les organismes ayant rédigé la présente ont déterminé que ces commandes étaient deux composants de maliciels associés à l'activité malveillante ciblant les dispositifs Cisco ASA sous les noms suivants :

- LINE RUNNER – un code encoquillé persistant permettant aux auteures et auteurs de menace de téléverser et d'exécuter des scripts Lua arbitraires;
- LINE DANCER – un implant en mémoire permettant aux auteures et auteurs de menace de téléverser et d'exécuter des charges de virus arbitraires dans le code de commandes.

Les organismes ayant rédigé la présente croient qu'il existe un lien entre ces composants en raison de l'utilisation temporaire des ressources partagées créées par l'auteure ou auteur de menace sur un dispositif touché.

On soupçonne que LINE RUNNER peut être présent sur un dispositif compromis même si LINE DANCER ne s'y trouve pas (par exemple, en tant que porte dérobée ou lorsque l'ASA touchée n'a pas encore reçu toute l'attention opérationnelle des auteures et auteurs de menace). Par conséquent, tout le travail de détection de LINE DANCER effectué précédemment et ayant donné lieu à des résultats négatifs ne signifie pas que LINE RUNNER n'est pas présent.

2.1 Requêtes HTTP (LINE RUNNER)

LINE RUNNER est un code encoquillé persistant basé sur Lua qui cible la fonctionnalité de personnalisation des dispositifs du client WebVPN sur l'appliance de sécurité adaptative (ASA) de Cisco. LINE RUNNER met en place plusieurs techniques d'évasion des défenses pour éviter la détection et prévenir la récupération lors d'investigations informatiques. LINE RUNNER permet d'exécuter le code Lua arbitraire envoyé par l'entremise de requêtes HTTP GET aux identificateurs de ressources uniformes (URI pour *Uniform Resource Identifier*) légitimes du WebVPN de Cisco ASA et de AnyConnect. Par exemple :

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

Où :

- <aaa> correspond au nom de clé d'un paramètre de requête randomisé;
- <token> correspond à une valeur randomisée vérifiée par le code encoquillé (c'est-à-dire, *auth*);
- <bbb> correspond au nom de clé d'un paramètre de requête randomisé;
- <lua_script> correspond aux commandes codées avec Lua de l'URL à exécuter.

L'utilisation de paramètres de requête randomisés empêche le balayage de masse des ASA potentiellement touchées. On suppose que les valeurs dans les requêtes GET sont déterminées en fonction des victimes, mais cela reste à confirmer.

2.2 Requête HTTP et réponse (LINE DANCER)

LINE DANCER est un chargeur de codes de commandes persistant basé sur Lua qui fait partie d'un cadriciel plus étendu. Ce chargeur de codes de commandes traiterait les charges de virus malveillantes qui exécutent des commandes système. LINE DANCER permet d'exécuter des charges de virus de codes de commandes, lesquelles sont décodées en Base64 et ne s'exécutent que lorsqu'elles sont placées par une valeur fixe de 32 bits, ce qui diffère d'une victime à l'autre. On retrouve ci-dessous un échantillon des requêtes HTTP POST envoyées aux URI du WebVPN de Cisco ASA et de AnyConnect :

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

…

<host-scan-reply>[charges de virus codées en base64]</host-scan-reply>
```

Pour aider les organisations dans leurs efforts de détection et d'atténuation, les organismes ayant rédigé la présente fournissent des échantillons supplémentaires des activités menées par les auteures et auteurs de menace :

- Les auteures et auteurs de menace ont généré des versions texte du fichier de configuration des dispositifs de manière à pouvoir les exfiltrer au moyen de demandes Web;
- Les auteures et auteurs de menace ont été en mesure de contrôler l'activation et la désactivation du service de journaux système sur les dispositifs et de dissimuler des commandes additionnelles;
- Les auteures et auteurs de menace ont été en mesure de modifier la configuration du protocole d'authentification, d'autorisation et de traçabilité (AAA pour *Authentication, Authorization and Accounting*) de manière à ce que les dispositifs sous leur contrôle correspondant à une identification en particulier puissent obtenir accès à l'environnement touché.

Cisco a attribué les vulnérabilités et expositions courantes (CVE pour *Common Vulnerabilities and Exposures*) suivantes à l'activité liée à LINE RUNNER [10] et à LINE DANCER [11] (en anglais seulement) :

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

On retrouve de l'information additionnelle sur ces vulnérabilités sur le portail des avis de sécurité de Cisco [7][8] et le blogue Cisco Talos [9] (en anglais seulement).

3 Indicateurs de compromission

3.1 Adresses IP

Les organismes ayant rédigé la présente ont observé que les adresses IP malveillantes ci-dessous ciblaient des réseaux. On peut considérer avec un degré élevé de certitude que ces adresses IP sont source d'activités malveillantes et il convient de rappeler aux organisations qu'elles ne doivent pas les sonder, mais plutôt vérifier les journaux du réseau pour d'importants volumes de données transférées. On devrait porter une attention particulière si ces adresses IP ont été observées entre décembre 2023 et février 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 Mesures recommandées

Les organismes ayant rédigé la présente ont été informés par Cisco que les plus récentes versions micrologicielles contenaient des correctifs pour aider à atténuer cette activité. Les correctifs inclus dans la mise à jour micrologicielle visent les techniques qui ont permis aux auteures et auteurs de menace de s'implanter en permanence au cours de la compromission. Les organisations sont invitées à surveiller les futurs articles et mises à jour micrologicielles de Cisco ainsi qu'à appliquer les correctifs nécessaires dès qu'ils sont diffusés.

Des correctifs peuvent actuellement être téléchargés sur le site Web de Cisco [5] au moyen d'un compte Cisco valide et moyennant un contrat actif de soutien avec Cisco pour les dispositifs ASA. Les organisations sont invitées à appliquer les plus récentes mises à jour qui pourraient contenir les correctifs propres à cette activité et d'autres mises à jour offertes pour le dispositif. Au moment de publier la présente, les plus récentes versions étaient les suivantes :

- 9.16.4.57
- 9.18.4.22
- 9.20.2.10

4.1 Instructions de mise à jour pour les dispositifs pris en charge

Cisco a fourni les instructions suivantes concernant le processus de mise à jour :

- consulter le centre de téléchargement de logiciels de Cisco au https://software.cisco.com/download/home/ (en anglais seulement);
- cliquer sur *Browse All*;
- sélectionner *Security > Firewalls*;
- selon la plateforme matérielle, sélectionner *3000 Series Industrial Security Appliances (ISA)*, *Adaptive Security Appliances (ASA)* ou *Next-Generation Firewalls (NGFW)*;
- sélectionner un produit précis dans le volet de droite du sélecteur de produit (selon la plateforme matérielle, il se peut que cette étape doive être répétée);
- sélectionner *Adaptive Security Appliance (ASA) Software*;
- aller à *All Release > Interim > 9 > 9.x.y Interim* (par exemple : 9.18.4 Interim). Remarque : Il est important de naviguer jusqu'à *Interim* en suivant les étapes ci-dessus pour trouver les versions appropriées.

4.2 Instructions de mise à jour pour les dispositifs non pris en charge

Pour tous les dispositifs qui ne sont plus pris en charge parce qu'ils ont atteint la fin de leur cycle de vie, les organisations devraient communiquer avec Cisco pour discuter de solutions de rechange. Les organismes ayant rédigé la présente souhaitent rappeler aux organisations l'importance de la gestion du cycle de vie des dispositifs. L'utilisation de logiciels ou de matériel désuets limite la capacité du fabricant de fournir des correctifs de sécurité.

Pour obtenir plus de conseils, veuillez communiquer avec votre équipe de soutien technique. S'il s'agit du centre d'assistance technique de Cisco (TAC pour *Technical Assistance Center*) de Cisco, veuillez consulter la pagehttps://www.cisco.com/c/fr_ca/support/index.html ou composer le 800-553-2447 (É.-U./Canada) pour ouvrir une demande d'assistance en utilisant le code de référence « **ARCANEDOOR** ». On peut trouver les numéros de téléphone internationaux sur le site Web de Cisco : https://www.cisco.com/c/fr_ca/support/web/tsd-cisco-worldwide-contacts.html

4.3 Recommandation pour une détection renforcée

Les organismes ayant rédigé la présente recommandent que les organisations prennent les mesures suivantes pour mieux se protéger et faciliter la détection des activités malveillantes :

1. Mettre à niveau les dispositifs exécutant un micrologiciel vulnérable à une version qui comprend les correctifs pertinents. L'exécution du plus récent micrologiciel fait en sorte que les dispositifs soient mieux protégés contre les vulnérabilités fraîchement découvertes.
2. Si aucun chemin d'accès n'est accessible pour le nouveau micrologiciel, mettre le dispositif hors service ou s'assurer que les services WebVPN sont désactivés.
3. Assurer la gestion adéquate du cycle de vie des logiciels et du matériel pour profiter du soutien et des mises à jour de sécurité du fabricant.
4. Depuis le 30 septembre 2019, Cisco n'offre plus de soutien pour WebVPN [6]. Si cette fonctionnalité est toujours utilisée, les organisations sont invitées à planifier la migration de la connectivité d'accès à distance vers une technologie prise en charge.
5. On invite les organisations à passer en revue les journaux pour filtrer les accès ou changements inconnus, non prévus ou non autorisés apportés sur les dispositifs. Les organisations devraient également surveiller les activités non prévues, comme les redémarrages impromptus, les transferts volumineux d'adresses IP inconnues et les lacunes dans la journalisation, puisque cela pourrait être signe de la désactivation des services de journalisation.
6. Activer la journalisation « informationnelle » sur tous les dispositifs Cisco ASA [1].
7. S'assurer que l'ouverture de session hors dispositif est suffisante pour prendre en charge l'analyse de l'historique, en particulier si la journalisation selon la sévérité a été augmentée dans les journaux système.
8. Vérifier auprès des administratrices et administrateurs si des codes d'alerte ont été observés afin de passer en revue l'activité malveillante potentielle.

Code de l'ASA	Descriptions (en anglais seulement)
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 Recommandations en matière de renforcement de la sécurité

Les recommandations en matière de renforcement de la sécurité suivantes empêcheront les auteures et auteurs de menace de mener des activités malveillantes en faisant appel aux tactiques, techniques et procédures (TTP) observées :

1. Désactiver ou limiter le trafic non chiffré interne acheminé par l'entremise des dispositifs passerelles, dont le trafic du bloc de messages de serveur (SMB pour *Server Message Block*). La version 3.0 ou plus récente du protocole SMB peut être configurée de manière à utiliser le chiffrement. Les versions antérieures du protocole SMB ne devraient pas être utilisées.
2. Renforcer l'accès en activant le protocole SNMPv3 et supprimer le protocole SNMPv2.
3. Des auteures et auteurs de menace pourraient exploiter les comptes et les justificatifs d'identité utilisés sur les dispositifs d'accès et intégrés aux systèmes internes, comme Active Directory. Les privilèges minimaux nécessaires devraient être accordés à ces comptes partagés pour que les auteurs et auteurs de menace ne puissent pas compromettre d'autres services. Ces comptes devraient être étroitement surveillés pour relever tout écart par rapport aux comportements attendus.
4. D'après les TTP observées, les organismes ayant rédigé la présente recommandent aux organisations d'exiger l'utilisation du protocole IPsec (*Internet Protocol Security*) plutôt que du protocole SSL/TLS (*Secure Socket Layer/Transport Layer Security*) en ce qui a trait à la connectivité au RPV. Les organisations devraient envisager de configurer tous les services de manière à bloquer l'accès public aux composants SSL du dispositif ASA [2][3].
5. S'il est nécessaire de mettre en place le protocole SSL/TLS du RPV ou d'autres services à accès externe, comme Secure Shell (SSH), les organisations devraient avoir recours aux plus récents protocoles sécurisés avec les suites de chiffrement recommandées et mettre en œuvre les mesures de renforcement de la sécurité fournies par le Centre pour la cybersécurité dans l'ITSP.40.062 [4].
6. Lorsque c'est possible, utiliser des listes de contrôle d'accès (LCA) pour bloquer l'accès externe au dispositif RVP à partir d'adresses IP qui sont connues comme étant malveillantes. Les LCA peuvent également être configurées de façon à autoriser l'accès depuis les pays à partir desquels les utilisatrices et utilisateurs distants sont censés se connecter; un processus que l'on appelle le « géoblocage ».
7. Avoir recours aux techniques de détection des menaces, à la collecte centralisée de journaux, à la gestion des informations et des événements de sécurité et à des mécanismes d'alerte et de signalement adéquats.

5 Références

Numéro	Référence
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 (en anglais seulement)
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 (en anglais seulement)
3	Device Security Guidance - Virtual Private Networks (VPNs) https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks (en anglais seulement)
4	Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062
5	Cisco Software Download https://software.cisco.com/download/home/ (en anglais seulement)
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 (en anglais seulement)
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 (en anglais seulement)
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 (en anglais seulement)
9	ArcaneDoor: New espionage-focused campaign targets perimeter network devices https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/ (en anglais seulement)
10	NCSC Malware Tipper - LINE RUNNER https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-runner.pdf (en anglais seulement)
11	NCSC Malware Tipper - LINE DANCER https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-dancer.pdf (en anglais seulement)