RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Date : 12 juin 2024
Version : 1.0
Nombre de pages : 9

FAILLES SUR LES ÉQUIPEMENTS DE SECURITE : RETOUR D'EXPERIENCE DU CERT-FR

L'année 2023 et le début de l'année 2024 ont été marqués par de nombreux incidents concernant des équipements de sécurité présents notamment en bordure de réseau. Ces incidents ont pour origine l'exploitation d'une ou plusieurs vulnérabilités critiques dans des pare-feux, passerelles VPN ou encore passerelles de filtrage au sens large :

- 12/06/2023 : vulnérabilité dans les produits Fortinet[1] ;
- 12/06/2023 : vulnérabilité dans Barracuda Email Security Gateway Appliance[2] ;
- 19/07/2023 : vulnérabilité dans Citrix Netscaler ADC et NetScaler Gateway[3] ;
- 23/10/2023 : vulnérabilité dans Citrix Netscaler ADC et NetScaler Gateway[4] ;
- 29/12/2023 : vulnérabilité dans Barracuda Email Security Gateway[5] ;
- 11/01/2024 : multiples vulnérabilités dans Ivanti Connect Secure et Policy Secure Gateways[6] ;
- 09/02/2024 : vulnérabilité dans Fortinet FortiOS[7] ;
- 12/04/2024 : vulnérabilité dans Palo Alto Networks GlobalProtect[8] ;
- 30/05/2024 : vulnérabilité dans les produits Check Point[9].

Compte tenu des impacts qu'ont eu les exploitations de ces vulnérabilités, le CERT-FR propose un retour d'expérience sur la gestion de ces vulnérabilités et des incidents associés.

[1] Cf. bulletin CERTFR-2023-ALE-004 : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-004/
[2] Cf. bulletin CERTFR-2023-ACT-025: https://www.cert.ssi.gouv.fr/actualite/CERTFR-2023-ACT-025/
[3] Cf. bulletin CERTFR-2023-ALE-008 : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-008/
[4] Cf. bulletin CERTFR-2023-ALE-012 : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-012/
[5] Cf. bulletin CERTFR-2024-ACT-001: https://cert.ssi.gouv.fr/actualite/CERTFR-2024-ACT-001/
[6] Cf. bulletin CERTFR-2024-ALE-001 : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-001/
[7] Cf. bulletin CERTFR-2024-ALE-004 : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-004/
[8] Cf. bulletin CERTFR-2024-ALE-006 : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-006/
[9] Cf. bulletin CERTFR-2024-ALE-008: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-008/ ,

DES CIBLES DE CHOIX

Le CERT-FR a, sur l'année 2023 et le début de l'année 2024 , en lien avec ce type d'équipements :

- publié 7 alertes et plus de 22 avis de sécurité ;
- réalisé plus d'une dizaine de campagnes de signalements relatives à l'identification d'équipements compromis, à des défauts de configuration ou bien encore à la présence de vulnérabilités, soit plusieurs dizaines de milliers signalements ;
- traité ou suivi le traitement de plus d'une centaine d'incidents, dont certains ont engendré la compromission intégrale du système d'information (SI) du bénéficiaire.

Ces dernières années, plusieurs vulnérabilités affectant ces équipements ont été activement exploitées d'abord de manière ciblée comme vulnérabilités dites « du jour zéro » (*zero day*). LE CERT-FR a pu confirmer le ciblage de ces équipements par des modes opératoires œuvrant au profit d'États à des fins d'espionnage ou encore à des fins de ciblage opportuniste en vue d'actions futures.

L'actualité de ces derniers mois a également mis en exergue une exploitation de plus en plus massive de ces vulnérabilités une fois révélées, soit par d'autres modes opératoires, soit plus globalement par des acteurs cybercriminels à des fins de déploiement de rançongiciel par exemple. Plusieurs jours, voire plusieurs semaines, ayant parfois été nécessaires aux constructeurs pour mettre à disposition des correctifs efficaces pour l'ensemble des modèles affectés, certaines vulnérabilités ont été exploitées massivement et à grande échelle, faute de mesures d'atténuation.

Malgré ces difficultés, le CERT-FR a relevé que plusieurs propriétaires d'équipements impactés ont, grâce à leur maturité SSI, leur veille active et leur réactivité, été en mesure de détecter des activités suspectes et ainsi pu réagir rapidement pour endiguer les tentatives de latéralisation, tout en tenant informé le CERT-FR des avancées de leurs investigations.

Par ailleurs, le CERT-FR a traité ces dernières années plusieurs cas de re-compromission de SI où la persistance du mode opératoire attaquant a été rendue possible grâce à son maintien dans ces équipements de bordure.

IMPORTANCE DES ÉQUIPEMENTS CONCERNÉS

Les SI modernes sont de taille parfois conséquente et reposent sur de nombreuses briques matérielles et logicielles. L'existence de vulnérabilités dans ces différentes briques, quelles qu'elles soient, est très difficilement évitable et doit donc être prise en compte.

Pour qu'un SI soit résilient, il doit être bâti de façon à permettre de résister à la défaillance d'une ou plusieurs de ses briques. Pour y parvenir, la mise en œuvre d'une sécurité dite "en profondeur" est nécessaire. La sécurité du SI ne doit pas reposer sur celle d'une seule brique, mais chaque brique doit être employée en considérant l'éventualité qu'elle (ou qu'une de ses briques adjacentes) puisse être

ciblée. L'identification, par exemple au travers d'une appréciation des risques, des briques les plus critiques et leur sécurisation au regard du reste du SI est donc un enjeu important, afin de rendre plus difficiles les chemins d'attaque jusqu'à celles-ci.

Le cloisonnement réseau est un des leviers efficaces pour la sécurisation d'un SI. Il vise à regrouper les portions d'un système d'information ayant des finalités communes et des niveaux de sécurité équivalents tout en les séparant des autres portions ayant des finalités et des enjeux de sécurité différents. Cette segmentation est également mise à profit au regard des différentes interconnexions possibles avec Internet. Elle permet ensuite de contrôler les flux autorisés à transiter entre différentes portions.

Pour mener à bien une segmentation, des équipements spécialisés sont souvent utilisés, notamment en raison de leur facilité d'intégration ainsi que des possibilités de centraliser les efforts de configuration et de maintenance. On citera les pare-feux, passerelles VPN, NAC, bastions, NIDS/NIPS - *sandbox*, passerelles antivirales, passerelles antispam-, etc. La nature, la finalité et l'image associée à ces équipements conduisent souvent à les placer, à tort, au-dessus de tout soupçon ou doute. Mais comme tout équipement déployé dans un système d'information, ces appareils sont des cibles. Chaque équipement déployé induit de nouveaux risques qui doivent être considérés : un équipement de sécurité est un serveur comme les autres. Ces briques de sécurité hébergent du code informatique pour fonctionner et, de ce fait, sont sujets aux vulnérabilités. Les incidents traités par le CERT-FR confirment qu'il s'agit même de cibles de choix.

IMPACTS DE L'EXPLOITATION DE VULNÉRABILITÉS SUR CES ÉQUIPEMENTS

Nombre de ces équipements proposent le regroupement de plusieurs fonctionnalités de sécurité au sein d'une même solution logicielle et matérielle, exposant une large surface fonctionnelle[10]. De plus, l'implémentation de ces fonctions est souvent basée sur des pratiques dépassées telles que :

- l'absence de compartimentation logique entre fonctions ;
- l'exécution des fonctions d'administration avec un compte hautement privilégié (voire administrateur) ;
- l'utilisation d'architectures et de cadriciels de développement Web obsolètes.

Du fait de leur position dans l'architecture interne, et, parfois, de leur adhérence à certaines parties critiques du SI (par exemple, des comptes privilégiés dans l'*Active Directory*), la compromission de ces équipements permet à un attaquant de compromettre en profondeur le SI et présente un risque fort qui n'est aujourd'hui pas suffisamment pris en compte.

[10] Telles que, par exemple, les pares-feux dits « nouvelle génération » (*Next Generation Firewall* ou *NGFW*)

Par ailleurs, plusieurs de ces solutions de filtrage offrent des services de configuration dynamique et automatisée en fonction des utilisateurs du SI. Pour ce faire, elles se reposent par exemple sur une intégration dans des annuaires, comme *Active Directory*, afin de récupérer les informations nécessaires à leur fonctionnement. Cette intégration peut être dangereuse pour la sécurité du SI lorsqu'elle impose l'octroi de droits privilégiés sur des contrôleurs de domaine, ou encore lorsqu'elle en hérite en raison d'une mauvaise procédure d'installation. En compromettant ces équipements, l'attaquant se retrouve alors en position de force car disposant, par héritage, des droits dont ces solutions disposent sur tout ou partie du SI.

Considérés comme des matériels et non des systèmes logiciels, de nombreux équipements fonctionnent en boîte noire. Ils ne disposent pas de mécanismes permettant un contrôle d'intégrité fiable, ni la réalisation de relevés de l'état de la mémoire et du système permettant de potentielles investigations numériques. Il est de plus généralement impossible pour leur propriétaire d'inspecter ou de superviser ces équipements, créant ainsi un « angle mort » dans la supervision de sécurité du SI.

Enfin, comme il est fréquent que les journaux produits par ces équipements ne soient pas, ou seulement partiellement, exportés vers des collecteurs de journaux, lorsqu'ils existent, leur authenticité n'est pas garantie lors des investigations numériques.

La remise en service d'un équipement compromis ou pour lequel un doute subsiste peut se révéler tout aussi complexe. C'est en particulier le cas quand la fonction de "remise en état d'usine" (*factory reset*) peut être altérée ou contournée. Un attaquant peut alors se maintenir sur l'équipement, même après que le plus haut niveau de réinitialisation disponible ait été effectué.

MESURES DE PRÉVENTION ET DE DURCISSEMENT D'INTÉGRATION

Au regard du rôle joué par ces équipements et solutions spécialisées, et en raison des défauts récurrents de sécurité observés pour nombre d'entre eux, un renforcement significatif de leur niveau de sécurité est déterminant. En particulier, le développement de fonctions de vérification d'intégrité, d'inspection système et de remise à zéro fiables est crucial.

Ainsi, de façon non limitative, le CERT-FR rappelle à ses bénéficiaires l'importance :

- dans la mesure du possible, d'utiliser des solutions évaluées au sens de la Certification de Sécurité de Premier Niveau ou des Critères Communs[11];
- de s'assurer que de tels équipements ne disposent pas de droits privilégiés, directs comme indirects, au sein des annuaires *Active Directory ou OpenLDAP* ou ne disposent pas de droits

[11] Pour plus de détails sur ces processus de certification et leurs apports cf. https://cyber.gouv.fr/comprendre-la-certification.

pouvant aboutir à l'exécution de code arbitraire sur des serveurs sensibles comme les contrôleurs de domaine ;

- de s'assurer au travers de leur inventaire qu'ils sont toujours maintenus par le constructeur ou l'éditeur et si ça n'est plus le cas, opérer un remplacement ;
- d'assurer une veille régulière sur les avis de sécurité relatifs à ces solutions et l'application des correctifs de sécurité dès que possible ;
- de contrôler régulièrement leur intégrité lorsque la solution le permet ;
- de mettre en œuvre autant que possible un déport automatisé des journaux et d'intégrer l'export des journaux système de ces équipements dans la supervision de sécurité de l'organisation ;
- de ne pas exposer les interfaces d'administration notamment sur Internet, mais aussi vers des réseaux non dédiés à l'administration de ces solutions ;
- d'utiliser les fonctions d'authentification multi-facteurs sur toutes les interfaces d'administration de ces équipements ;
- de désactiver les fonctionnalités non indispensables lorsque la solution le permet ;
- dans la mesure du possible et sans compromettre le maintien en condition opérationnelle et de sécurité, de dédier un équipement à une fonctionnalité ;
- de considérer que la simple application du correctif puisse ne pas avoir été suffisante en cas compromission ou de suspicion de compromission et, sauf engagement contraire formel du constructeur, d'envisager une investigation numérique avant une restauration d'usine et un renouvellement de l'ensemble des secrets dont disposait la solution.

Sur ce dernier point, il est essentiel de réaliser que l'application d'un correctif de sécurité tend à corriger la vulnérabilité avant une tentative de compromission, **mais ne supprime pas une persistance si elle a déjà été implantée après une compromission**.

PROCHAINES ÉTAPES

Les évolutions législatives en cours, aussi bien européennes (notamment : l'article 12 de la directive NIS2[12], l'article 56, alinéa 8 du CSA[13], l'article 10 de la proposition de règlement CRA[14]) que nationales (article L2321-4-1 du Code de la défense) créent de nouvelles obligations à la charge des éditeurs qui doivent permettre d'améliorer le niveau de sécurité des produits et, *in fine*, contribuer à réduire ce type d'incidents. L'ANSSI est pleinement engagée sur ces sujets et veillera à son échelle à la mise en œuvre et au respect de ces obligations.

---

[12] *Network and Information Security Directive* : Directive UE 2022/2555 du 14 décembre 2022. Pour plus d'informations sur cette directive, cf. https://cyber.gouv.fr/la-directive-nis-2.

[13] *Cybersecurity Act* : Règlement UE 2019/881 du 17 avril 2019. Pour plus d'informations sur ce règlement cf. https://cyber.gouv.fr/cybersecurity-act.

[14] *European Cyber Resilience Act* : Proposition de règlement du parlement européen et du conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement UE 2019/1020. Pour plus d'informations sur cette proposition de règlement cf. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

QUE FAIRE EN CAS DE COMPROMISSION ?

En cas de compromission ou de suspicion de compromission, le CERT-FR vous invite à prendre connaissance de cette page :
https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/

Le CERT-FR est joignable :

- **Par téléphone :**
  - depuis la France métropolitaine au *3218* (service gratuit + prix d'un appel) ou *09 70 83 32 18*
  - depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au *+33 9 70 83 32 18*
- **Par courriel** :
  - à l'adresse *cert-fr@ssi.gouv.fr*

POUR ALLER PLUS LOIN

- https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/
- https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/
- https://www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/
- https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation
- https://cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique

ANNEXE

Synthèse sommaire de quelques vulnérabilités ayant affecté des concentrateurs VPN SSL

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-006/
  - **Système affecté :** Palo Alto GlobalProtect
  - **Chemin d'attaque observé :** au niveau d'une interface Web, le fonctionnement du cookie de session implique l'écriture d'un fichier dans */tmp* avec comme nom le contenu du cookie. Il existe une injection dans le cookie de session (SESSID) qui permet de créer un fichier à un chemin arbitraire sur le système (en tant que *root*). Une méthode d'exploitation consiste en l'injection de commande dans le service de télémétrie à partir de ce nom de fichier. En effet, ce service construit la commande en concaténant le nom du fichier. En pratique cette injection a été utilisée pour télécharger un fichier malveillant ou pour exposer les fichiers de configuration critiques du système.
    - **Note :** le service de télémétrie est celui qui a été exploité ; cependant d'autres vecteurs d'exploitation semblent possibles (l'éditeur a supprimé la mesure de contournement consistant à désactiver le service et a plus tard confirmé que d'autres vecteurs existent)
  - **Facilité d'exploitation :** très simple.

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-004/
  - **Systèmes affectés :** FortiOS et FortiProxy SSL VPN
  - **Chemin d'attaque observé :** écriture hors limite sur la pile de deux octets (0x0a0d) à cause d'une mauvaise gestion d'un paramètre de taille dans l'option *Chunked transfer Encoding* HTTP. La position de l'écriture est partiellement maîtrisée et permet notamment d'écrire après le canari de la pile (*stack canary*). L'exploitation proposée repose sur la réécriture de variables locales correspondant à des pointeurs vers le tas et donc à des manipulations de la structure du tas.
  - **Facilité d'exploitation :** difficile.

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-001/
  - **Systèmes affectés :** Ivanti Connect Secure, Ivanti Policy Secure Gateways, Ivanti Neurons pour passerelles ZTA
  - **Chemin d'attaque observé :**
    - CVE-2023-46805 : contournement d'authentification en utilisant une règle qui ne demande pas d'authentification si le début de la route demandée correspond à une certaine valeur (*/api/v1/totp/user-backup-code,*) puis en

complétant la route par une traversée arbitraire du système de fichier ("*path traversal*"). Cette construction d'URLpermet par la suite de demander l'accès à une autre route (par exemple */api/v1/totp/user-backup-code/../../system /system-information*)

- CVE-2024-21887 : plusieurs routes d'*API* (authentifiées) injectent directement des données HTTP dans la commande python sous-jacente *Popen* : *api/v1/totp/user-backup-code/../../license/keys-status/;CMD;* où CMD est la commande à exécuter.
- CVE-2024-21893 : attaque basée sur l'injection de requêtes illégitimes par rebond côté serveur (*Server Side Request Forgery*, *SSRF)* dans une route accessible sans authentification qui repose sur une vulnérabilité « N-day » (6 mois de retard environ) affectant le composant *xmltooling*
- CVE-2024-22024 : Une vulnérabilité permet un injection d'entité externe XML (*XML eXternal Entity*, *XXE*) basique directement exploitable (encodée en base64) depuis une requête POST sur une route ne demandant pas d'authentification. La vulnérabilité a été introduite en corrigeant la vulnérabilité précédente.

- **Facilité d'exploitation :** très simple.

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-012/
  - **Systèmes affectés :** Citrix NetScaler ADC et NetScaler Gateway
  - **Chemin d'attaque observé :** lecture de mémoire hors limite s'appuyant sur la mauvaise gestion d'une taille de tampon. La taille de tampon est calculée à partir du retour de la fonction *snprintf* cependant cette fonction retourne la taille totale et non pas la taille écrite. La lecture suivante peut donc lire des données hors du tampon. Il est possible d'utiliser le contenu de l'en-tête Host avec une taille importante pour obtenir des données stockées en dehors du tampon. En particulier, selon les instances, un jeton d'authentification peut être retrouvé parmi les données.
  - **Facilité d'exploitation :** simple.

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-008/
  - **Systèmes affectés :** Citrix ADC et NetScaler Gateway
  - **Chemin d'attaque observé :** débordement de tampon dans la pile en passant un paramètre (*target*) de taille supérieure à *0x80* sur une route accessible sans authentification (*/gwtest/formssso?event=start&target=AAAAAAAAAAAAAAAA[...]*)
  - **Facilité d'exploitation :** moyen, le binaire ne bénéficie d'aucun des mécanismes de protection contre les débordements de tampon (*Address Space Layout Randomization*, *ASLR*, *Data Execution Prevention*,*DEP* et *stack canary*).

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-004/
  - **Systèmes affectés :** FortiOS et FortiProxy SSL VPN
  - **Chemin d'attaque observé :** une route HTTP accepte un paramètre *enc* (non utilisé sur les versions récentes du produit) dont le contenu est chiffré par un mécanisme basé sur XOR à l'aide d'une séquence de clés. Cette séquence repose sur le calcul de condensats *md5* successifs en partant d'une clé fournie dans les 4 premiers octets et d'un sel récupérable sur une autre route. La taille du paramètre est également fournie par l'utilisateur. Une vérification de cette taille par rapport à la taille du tampon alloué est réalisée de manière incorrecte et permet donc de dépasser la limite du tampon, qui est stocké sur la pile. Il ne s'agit pas d'une simple écriture en dehors du tampon puisque le contenu (dans et hors du tampon) est déchiffré par l'application. L'exploitation requiert donc d'exploiter un *xor* de mémoire avec des valeurs de md5.
  - **Facilité d'exploitation :** difficile à très difficile, toutefois l'allocateur mémoire utilisé permet de façon exotique de simplifier l'exploitation.