Top 10 des vulnérabilités de 2021

RÉSUMÉ

Table des matières

1 Introduction

Ce document propose une analyse des vulnérabilités les plus critiques traitées par l'ANSSI au cours de l'année 2021. Cette démarche s'inscrit dans les missions de sécurité et de défense des systèmes d'information de l'agence, et en particulier la mission de veille et d'information sur les vulnérabilités.

Malgré une adoption progressive des techniques et bonnes pratiques de développement sécurisé, il est impossible de garantir qu'un produit soit totalement exempt de vulnérabilités. La découverte d'une vulnérabilité fait partie intégrante du cycle de vie d'un produit. Les vulnérabilités non corrigées sont susceptibles d'être exploitées par des attaquants afin de réaliser des actions malveillantes et de compromettre des équipements. Ainsi, il est essentiel d'appliquer les correctifs proposés par les éditeurs de solutions.

Au-delà des vulnérabilités décrites dans ce document, l'ANSSI rappelle qu'il est vital, pour le maintien en condition de sécurité des systèmes d'information, d'assurer une veille constante sur les vulnérabilités découvertes et publiées quotidiennement sur Internet. La grande majorité des éditeurs de solutions proposent des avis de sécurité afin de prévenir des nouvelles vulnérabilités affectant leurs produits. Par ailleurs, par le biais du CERT-FR, l'agence propose aussi un service de veille quotidienne sur une liste de produits largement utilisés sur le territoire Français [1].

2 Constats généraux sur les vulnérabilités

En 2021, l'ANSSI, à travers le CERT-FR, a publié 991 avis et 22 alertes concernant des vulnérabilités dans les produits suivis par l'agence. Par ailleurs, 31 campagnes de signalement ont été menées vers les entités publiques et privées identifiées comme exposant des services ou équipements vulnérables [1].

Cette année fut notamment marquée par plusieurs vulnérabilités corrigées dans le service de messagerie Microsoft Exchange Server et qui peuvent être exploitées à travers l'interface Web Outlook Web Access (*OWA*). L'éditeur propose régulièrement des correctifs de sécurité (*Security Update*) qui peuvent être appliqués uniquement sur les deux dernières mises à jour « cumulatives »(*Cumulative Update*, *CU*). Il est donc primordial de procéder régulièrement à la mise à jour des serveurs Microsoft Exchange pour être en mesure d'appliquer les correctifs de sécurité lors de leur mise à disposition par l'éditeur. Cette recommandation est particulièrement importante car les serveurs Exchange étant fortement couplés avec Active Directory , le risque qu'une vulnérabilité dans ce produit puisse permettre de compromettre l'infrastructure Active Directory du système d'information est très élevé.

1. https://www.cert.ssi.gouv.fr/avis/

Plusieurs vulnérabilités ont également affecté des services utilisés dans le cadre de projets de développement logiciel tels que GitLab et Atlassian Confluence . Ces vulnérabilités critiques ont pu être exploitées parce que ces services sont trop souvent exposés directement sur Internet [2]. Il est pourtant essentiel de protéger les infrastructures de développement logiciel, comme l'ont démontré des incidents tels que la compromission en masse du logiciel SolarWinds Orion fin 2020.

Une des mesures recommandées pour sécuriser l'accès au système d'information depuis un réseau externe consiste à mettre en place un réseau privé virtuel (*Virtual Private Network*, *VPN*). Les passerelles VPN permettant de sécuriser l'accès au système d'information depuis l'extérieur sont dès lors des équipements critiques. Les mises à jour de sécurité doivent être appliquées rapidement, tandis que la robustesse du dispositif doit notamment être assurée par l'utilisation de mécanismes cryptographiques robustes, la mise en place d'une politique de journalisation adéquate ainsi qu'une politique de contrôle d'accès basée sur une authentification multi-facteurs[2].

Par ailleurs, il est encore fréquent d'observer la présence d'interfaces d'administration accessibles sur Internet et faiblement sécurisées. Dans certains cas, le fait que ces interfaces soient directement exposées sur Internet n'est pas connu de l'organisation car celles-ci sont parfois configurées par défaut et qu'aucun contrôle de sécurité (*scan*, audit) n'est réalisé pour les détecter. Dans d'autre cas, les besoins d'administration à distance n'ont pas été couverts par une infrastructure sécurisée adaptée permettant de limiter l'exposition aux équipements [3].

L'année 2021 aura également vu la découverte de différentes failles dans certains services et protocoles Microsoft . Ces failles peuvent permettre aux attaquants de prendre le contrôle du domaine *Active Directory* rapidement lorsque les bonnes pratiques de sécurisation ne sont pas correctement appliquées [4]. Il est ainsi possible de mentionner les vulnérabilités dans le service d'impression (*Printnightmare*) ou encore la possibilité d'utiliser le protocole d'authentification NTLM pour élever ses privilèges (avec un outil tel que *PetitPotam*).

Enfin, il est difficile de résumer l'année 2021 sans évoquer les vulnérabilités découvertes dans la bibliothèque Javalog4j . Ce cas de figure résume à lui seul toute la difficulté que peut représenter la gestion des dépendances entre logiciels.

2. Pour en savoir plus sur les bonnes pratiques en matière de protection des services exposés sur Internet, voir [2]

3. Pour en savoir plus sur les bonnes pratiques en matière d'administration des systèmes d'information, voir [3] et [4]

4. Pour en savoir plus sur les bonnes pratiques en matière de gestion des environnements Microsoft, voir [5], [6] et [7]

Certains éditeurs continuent en effet de mettre à jour leurs produits en 2022 pour des vulnérabilités pourtant découvertes il y a plusieurs années. C'est par exemple le cas de la CVE-2020-36179 qui affecte la bibliothèque d'interprétation du format XML Jackson et a un score CVSSv3 de 8,8. Cette dernière permet à un attaquant d'exécuter du code arbitraire à distance, lorsque les conditions d'utilisation de cette bibliothèque au sein d'un produit le permettent. Cette vulnérabilité a récemment fait l'objet de correctifs par des éditeurs comme Oracle ou IBM .

L'identification des dépendances au sein d'un logiciel répond au même impératif qu'une cartographie du système d'information : être en mesure de répondre rapidement à la découverte d'une vulnérabilité après une analyse de risques.

3 Les 10 vulnérabilités les plus marquantes de 2021

L'identification d'une ou plusieurs vulnérabilités dans des équipements exposés sur Internet est l'une des méthodes les plus communes pour l'accès initial à un système d'information, mais également pour y obtenir des privilèges élevés. Les vulnérabilités présentées dans ce document ont été sélectionnées en fonction de leur criticité et des cas d'exploitation observés. Ont été privilégiées dans cette sélection les vulnérabilités permettant une primo-intrusion sur le réseau informatique, et celles ayant un impact critique sur le système d'information dans son ensemble.

3.1 CVE-2021-26855 – « ProxyLogon »

Le 2 mars 2021, Microsoft a publié des correctifs concernant des vulnérabilités critiques de type « jour zéro » (*zero day*) affectant les serveurs de messagerie Exchange en versions 2010, 2013, 2016 et 2019. Ces vulnérabilités permettent à un attaquant de réaliser une exécution de code arbitraire à distance, permettant d'obtenir in fine les droits de l'administrateur de domaine *Active Directory*.

- CVE-2021-26855 : Aussi nommée *ProxyLogon*, il s'agit d'une vulnérabilité côté serveur de type *SSRF* permettant à l'attaquant non authentifié d'envoyer des requêtes HTTP arbitraires qui seront exécutées sous l'identité du serveur Exchange .
- CVE-2021-27065 : Vulnérabilité post-authentification permettant à l'attaquant de pouvoir écrire un contenu arbitraire dans un fichier. Les droits d'accès peuvent être obtenus soit en exploitant la CVE-2021-26855, soit en compromettant les identifiants d'un administrateur légitime.
- CVE-2021-26857 : Vulnérabilité basée sur une faiblesse de la désérialisation dans le service de messagerie unifiée (*Unified Messaging*). Cette vulnérabilité permet à l'attaquant de pouvoir exécuter du code arbitraire à distance avec les privilèges SYSTEM sur le serveur Exchange . L'exploitation de cette vulnérabilité demande les droits administrateurs (ou l'exploitation d'une autre vulnérabilité).

- CVE-2021-26858 : Vulnérabilité post-authentification permettant à l'attaquant de pouvoir écrire un contenu arbitraire dans un fichier. Les droits d'accès peuvent être obtenus soit en exploitant la CVE-2021-26855 soit en compromettant les identifiants d'un administrateur légitime.

Ces vulnérabilités ont été largement exploitées dans des attaques ciblées qui ont notamment été attribuées à un mode opératoire d'attaque dénommé *Hafnium* par Microsoft [8]. En complément, les chercheurs de Volexity [9] indiquent avoir détecté des premières attaques dès janvier 2021.

Référence : [10].

3.2 CVE-2021-31207 – « ProxyShell »

Le jeudi 5 août 2021, le chercheur en sécurité OrangeTsai dévoilait plus de détails concernant trois vulnérabilités déjà connues [11] qui, lorsqu'elles sont exploitées en chaîne, permettent de prendre le contrôle d'un serveur Exchange à distance. Ces vulnérabilités, regroupées sous le nom de *ProxyShell*, sont les suivantes :

- CVE-2021-34473 : Permet à un attaquant non authentifié de contourner les listes de contrôle d'accès (ACL) ;
- CVE-2021-34523 : Permet à un attaquant d'élever ses privilèges ;
- CVE-2021-31207 : Permet à un attaquant une écriture de fichier arbitraire, ce qui conduit à une exécution de code arbitraire à distance.

Le CERT-FR a eu connaissance de campagnes de recherches actives sur Internet ciblant les serveurs Exchange pour ces vulnérabilités. Les correctifs pour les vulnérabilités CVE-2021-34473 et CVE-2021-34523 ont été publiés par Microsoft en avril 2021. Toutefois l'éditeur ne les a publiquement annoncés qu'à l'occasion de sa mise à jour de juillet 2021. La vulnérabilité CVE-2021-31207 a quant à elle été corrigée en mai 2021.

Référence : [12]

3.3 CVE-2021-26084 – Confluence

Le 25 août 2021, Atlassian a publié un avis de sécurité alertant de l'existence d'une vulnérabilité affectant la solution de travail collaboratif Confluence .

La vulnérabilité référencée CVE-2021-26084 a un score CVSS de 9.8. Elle permet à un attaquant non authentifié d'exécuter du code arbitraire à distance. L'éditeur a indiqué que cette vulnérabilité a été activement exploitée.

Le CERT-FR a également eu connaissance de campagnes d'identification de serveurs Confluence exposés sur Internet. Des codes d'exploitation sont disponibles publiquement pour cette vulnérabilité.

Référence : [13].

3.4 CVE-2021-22205 – Gitlab

Le 14 avril 2021, l'éditeur GITLAB déclarait que de multiples vulnérabilités avaient été découvertes dans ses produits. L'une d'elles, la CVE-2021-22205, permet à un attaquant non authentifié de provoquer une exécution de code arbitraire à distance. Son score CVSSv3 s'élève à 9.9. Les produits concernés sont GITLAB COMMUNITY EDITION et GITLAB ENTERPRISE EDITION .

Le CERT-FR a eu connaissance de codes d'exploitation disponibles publiquement dès juin 2021. Cette vulnérabilité a été activement exploitée car de nombreux services étaient exposés sur Internet.

Référence : [14].

3.5 CVE-2021-22893 – Pulse Secure

Le 20 avril 2021, PULSE SECURE a publié un bulletin de sécurité concernant la vulnérabilité CVE-2021-22893. Cette vulnérabilité, d'un score CVSSv3 de 10, permet à un attaquant non authentifié d'exécuter du code arbitraire à distance.

La vulnérabilité a été activement exploitée dès la publication de l'avis éditeur et dans le cadre d'attaques ciblées. Au cours d'une exploitation réussie, les attaquants modifient certains fichiers pour déposer des portes dérobées et effacer leurs traces.

Le 3 mai, l'éditeur a publié le correctif pour la vulnérabilité CVE-2021-22893, ainsi que les vulnérabilités CVE-2021-22894, CVE-2021-22899 et CVE-2021-22900 ayant un score CVSSv3 de 9.9, 9.9 et 7.2.

Référence : [15].

3.6 CVE-2021-20016 – SonicWall

Le 1er février 2021, SONICWALL a confirmé l'existence d'une vulnérabilité dans les passerelles d'accès sécurisé SMA SERIE 100 .

Cette vulnérabilité a pour identifiant CVE-2021-20016 et a un score CVSSv3 de 9.8. Elle permet à un attaquant non authentifié d'obtenir des informations de connexion, en particulier celles des comptes administrateurs. L'attaquant peut alors prendre la main sur l'équipement avec les privilèges les plus élevés.

Le 03 février 2021, puis le 19 février 2021, SONICWALL a publié deux correctifs pour la vulnérabilité CVE-2021-20016. Dans son communiqué, l'éditeur indique que le second correctif contient des mesures de durcissement du code et invite ses clients à l'installer immédiatement. Il confirme également l'obligation de changer tous les mots de passe une fois ce correctif appliqué.

Le 29 avril 2021, FIREEYE [17] fait état de l'exploitation de la vulnérabilité CVE-2021-20016 par un groupe cybercriminel dans le but de déployer plusieurs rançongiciels à l'encontre de différentes entités en Europe et en Amérique du Nord.

Référence : [16].

3.7 CVE-2021-22986 – F5

Le 11 mars 2021, l'éditeur F5 Networks annonçait plusieurs vulnérabilités affectant le produit BIG-IP, dont la vulnérabilité désignée par l'identifiant CVE-2021-22986 avec un score CVSSv3.1 de 9.8.

Il s'agit d'une vulnérabilité de type *SSRF* (*Server Side Request Forgery*) sur l'interface de programmation (*API*) REST des équipements BIG-IP de F5 . Elle permet à un attaquant non authentifié de provoquer une exécution de code arbitraire à distance.

Cette *API* permet l'automatisation de certaines tâches d'administration. Elle est accessible depuis l'interface d'administration de l'équipement mais également depuis les adresses IP dénommées *self-IPs* qui peuvent être configurées dans les différents *VLANs* auxquels ces équipements sont connectés.

Référence : [18].

3.8 CVE-2021-21985 – VMware

Le 25 mai 2021, VMware a publié un correctif pour la vulnérabilité CVE-2021-21985 affectant le greffon Virtual SAN Health Check qui est installé par défaut dans vCenter Server .

L'exploitation de cette vulnérabilité permet à un attaquant non authentifié d'exécuter du code arbitraire à distance avec un haut niveau de privilèges. De plus, des codes d'attaque sont disponibles publiquement pour la vulnérabilité CVE-2021-21985 et le CERT-FR a connaissance d'exploitations actives de celle-ci.

Référence : [19]

3.9 CVE-2021-34527 – « PrintNightmare »

Le 29 juin 2021, deux chercheurs ont présenté une vulnérabilité, la CVE-2021-34527 aussi nommée *PrintNightmare*, affectant le spouleur d'impression (*print spooler*) qui est un composant du système d'exploitation Windows activé par défaut. Elle permet à un attaquant d'exécuter du code arbitraire à distance avec les droits SYSTEM. Cette vulnérabilité fait suite à la CVE-2021-1675 initialement corrigée lors du *Patch Tuesday* du 9 juin 2021 et qui affecte le même composant.

Des codes d'exploitation pour cette vulnérabilité ont été rapidement rendus disponibles sur Internet. Ils exploitent la possibilité offerte par le service spouleur d'impression de téléverser un pilote dans le cadre de l'ajout d'une nouvelle imprimante pour installer un code malveillant. Ce service étant activé par défaut, tout système Windows est donc vulnérable avec la possibilité d'une exploitation à distance.

En particulier, au sein d'un système d'information Microsoft , les contrôleurs de domaine Active Directory sont particulièrement exposés, puisqu'un attaquant, en ayant préalablement compromis un poste utilisateur, pourra *in fine* obtenir les droits et privilèges de niveau « administrateur de domaine »Active Directory .

Référence : [20].

3.10 CVE-2021-44228 – « Log4Shell »

Le 10 décembre 2021, l'éditeur Apache a émis un avis de sécurité concernant la bibliothèque de journalisation Log4j . Cette bibliothèque est très souvent utilisée dans les projets de développement d'application Java/J2EE ainsi que par les éditeurs de solutions logicielles sur étagère basées sur ces technologies.

Cette vulnérabilité, avec un score CVSSv3 de 10 sur 10, permet à un attaquant de provoquer une exécution de code arbitraire à distance s'il a la capacité de soumettre une donnée à une application qui utilise la bibliothèque Log4j pour journaliser l'évènement. Cette attaque peut être réalisée sans être authentifié, par exemple en tirant parti d'une page d'authentification qui journalise les erreurs d'authentification.

Elle fait toujours l'objet d'une exploitation active, en particulier vis-à-vis des serveurs Web VMware Horizon exposés.

La vulnérabilité principale aura nécessité plusieurs correctifs successifs car des possibilités d'exploitation dans des contextes légèrement différents ont été découvertes par la suite. Ce fut le cas du contexte d'exploitation des vulnérabilités ayant les identifiants CVE-2021-45046, CVE-2021-45105 et CVE-2021-44832. Ces trois vulnérabilités ont été corrigées dans la version Log4j 2.17.1.

Les vulnérabilités concernant la version 1.x de la bibliothèque et identifiées par CVE-2022-23302, CVE-2022-23305 et CVE-2022-23307 ne seront pas corrigées par l'éditeur. Ce dernier indique que la version 1.2 est arrivé en fin de vie en août 2015. Les nouvelles versions de Log4j v2.x gèrent désormais les directives de configuration Log4j v1.x. La migration est ainsi simplifiée, et le CERT-FR encourage fortement les utilisateurs de Log4j v1.x à mettre à jour vers les versions 2 les plus récentes.

Référence : [21].

4 Le rôle de ces vulnérabilités dans les incidents de sécurité

4.1 Préambule

Ce chapitre n'est pas une représentation exhaustive de la réalité des événements de sécurité en lien avec l'exploitation d'une vulnérabilité. Cet état de la situation est dressé uniquement sur la base des incidents traités par l'ANSSI. Ainsi, la vision qui en résulte est partielle, et repose sur les sollicitations des bénéficiaires et l'initiative de partenaires à signaler ces événements.

Il convient également de rappeler le biais induit par la variété des systèmes et équipements analysés dans le processus d'identification de l'exploitation d'une vulnérabilité, ainsi que les contraintes de temps. En effet, les outils ainsi que les conditions d'investigation ne sont pas toujours réunis pour permettre une analyse approfondie des équipements et systèmes concernés par l'incident.

4.2 Principales vulnérabilités explicitement identifiées

Pour les événements de sécurité numérique affectant les entreprises et entités publiques françaises ayant été traités par l'ANSSI entre le 1er janvier 2020 et le 30 septembre 2021, il est possible de retenir les faits suivants :

- Certaines vulnérabilités pourtant anciennes restent toujours exploitées parce que les propriétaires de ces produits ne les mettent pas à jour. Ainsi, plusieurs incidents auront été causés par l'exploitation de la CVE-2018-13379 affectant les équipements VPN-SSL de FORTINET pour laquelle un correctif existe depuis le 24 mai 2019.
- Les équipements VPN de marque PULSE SECURE ont également été ciblés, notamment avec l'exploitation de la CVE-2021-22893 évoquée précédemment. Points d'entrée des réseaux internes, ces équipements doivent être surveillés et maintenus à jour.
- Des serveurs VMWARE VSPHERE exposés sur Internet ont été pris pour cible par des attaquants qui ont exploités la CVE-2021-21985 présentée ci-dessus.
- Enfin, beaucoup d'incidents ont été liés à l'exploitation des vulnérabilités rassemblées sous le nom de *ProxyLogon* et affectant MICROSOFT EXCHANGE .
- Le CERT-FR avait publié une alerté et réalisé au moins une campagne de signalement pour chacune de ces vulnérabilités afin de prévenir les entités exposant un équipement potentiellement vulnérable.

5 Etude de cas : Microsoft Exchange « ProxyLogon »

L'ANSSI a traité plusieurs dizaines d'incidents durant lesquels ces vulnérabilités ont été exploitées.

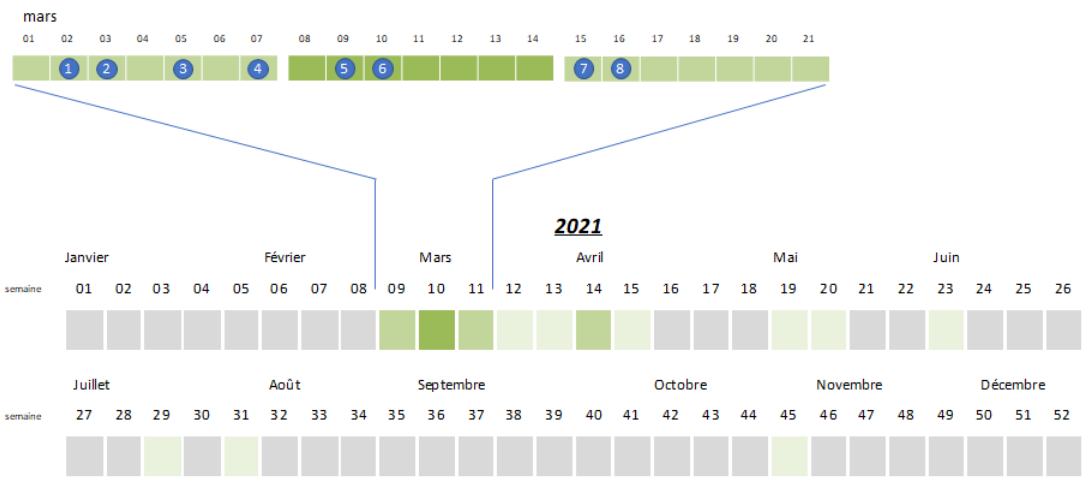

Figure 1 – Chronologie des signalements d'incidents liés à *ProxyLogon*, et les évènements notables associés. Le volume de signalements est représenté par l'intensité de la couleur verte.

Les évènements notables mentionnés dans la Figure 1 sont les suivants.

1. Le 2 mars, l'éditeur publie un avis en dehors du cycle normal de publication (*Patch Tuesday*), qui indique que ces vulnérabilités font déjà l'objet d'une exploitation dans des attaques ciblées. Dans ce contexte, l'ANSSI a activé à la fois une démarche de recherche des équipements vulnérables afin d'aider à l'identification des victimes potentielles ainsi qu'une préparation à la réponse à incidents.
2. Le CERT-FR émet une alerte (CERTFR-2021-ALE-004) afin de recommander la déconnexion immédiate des serveurs d'Internet, puis l'analyse des serveurs pour la recherche de compromission (sur la base des indicateurs de compromission publiés par l'éditeur et par Volexity) et enfin leur mise à jour. Les premiers incidents sont signalés immédiatement après la publication des informations sur l'existence des vulnérabilités.
3. Le CERT-FR effectue une campagne de signalement vers les entités exposant des serveurs Exchange vulnérables afin d'accélérer la prise en compte de la gravité de la situation.
4. Microsoft met à disposition un outil permettant la détection de l'exploitation des vulnérabilités sur la base des premiers indicateurs de compromissions. Le CERT-FR met à jour son alerte en conséquence.
5. Le CERT-FR met à jour son alerte après avoir fait le constat qu'environ 70% des serveurs identifiés ne sont pas dans une version permettant leur mise à jour avec les correctifs de sécurité proposés par Microsoft . Beaucoup d'entités sont ainsi contraintes d'appliquer la dernière mise à jour cumulative avant de pouvoir appliquer les correctifs.
6. Le CERT-FR émet une note aux opérateurs d'importance vitale (OIV) et aux opérateurs de services essentiels (OSE) demandant la mise en oeuvre des mesures de protection sans délai.
7. Une seconde campagne de signalement à destination des entités exposant un ou plusieurs serveurs Exchange vulnérables est réalisée.

Le nombre maximal de signalements fut atteint en semaine 10, mais des incidents ont été signalés jusqu'en semaine 14 (5-10 avril 2021) principalement, indiquant que les bénéficiaires avaient engagé leur plan d'action rapidement face à la gravité de la situation mais que les investigations pouvaient être longues. Par la suite, différents incidents ont été remontés mais en plus faible nombre.

En juin 2021, environ 5% des serveurs Exchange identifiés par l'ANSSI étaient encore vulnérables (ou potentiellement vulnérables) à *ProxyLogon*, ce qui constitue néanmoins une nette amélioration par rapport à la situation initiale.

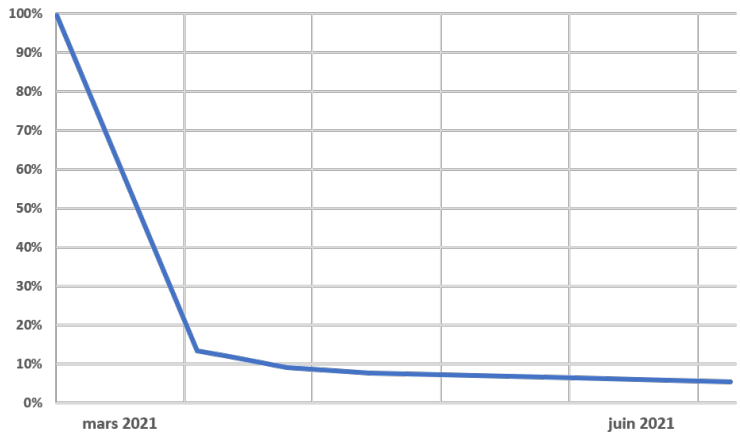

Figure 2 – Nombre de serveurs en France identifiés par le CERT-FR comme vulnérables à *ProxyLogon*. La majorité d'entre eux ont été mis à jour dans les premières semaines suivant la publication de la vulnérabilité, mais certains équipements étaient toujours vulnérables plusieurs mois plus tard.

Il est certain que le travail de mise à jour des serveurs Exchange aura facilité l'application des correctifs pour la vulnérabilité *ProxyShell* révélée en juillet 2021.

6 Conclusion

En 2021, de nombreux incidents sont liés à l'exploitation de l'une des vulnérabilités ayant fait l'objet d'avis ou d'alerte CERT-FR ainsi que de campagnes de signalement.

La gestion des vulnérabilités doit faire partie intégrante des prestations techniques pour le maintien en condition de sécurité des systèmes d'information, car il n'existera jamais de logiciel invulnérable. La mise à jour d'un produit ou d'un logiciel est une opération délicate qui doit être menée avec prudence. Des dispositions doivent également être prises pour garantir la continuité de service en cas de difficultés lors de l'application des mises à jour comme des correctifs ou des changements de version. C'est pourquoi l'ANSSI recommande d'intégrer le déploiement des correctifs de sécurité dans les processus de production (gestion des configurations, gestion des changements, gestion des incidents, etc.) afin d'en systématiser l'application selon une politique clairement établie par les parties prenantes (responsable de production et responsable de la sécurité).

La mise à jour du système d'information est une mesure très importante des 42 mesures du guide d'hygiène informatique publié par l'ANSSI, voir [22].

Pour suivre les publications du CERT-FR :

- https ://www.cert.ssi.gouv.fr/
- Twitter : @CERT_FR

Références

[1] Retour d'expérience sur les campagnes de signalement : https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-022/

[2] Recommandations sur le nomadisme numérique : https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

[3] Sécuriser l'administration des systèmes d'information : https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/

[4] https://www.ssi.gouv.fr/uploads/2020/06/anssi-guide-passerelle_internet_securisee-v3.pdf

[5] Recommandations de sécurité relatives à Active Directory : https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

[6] Durcissement et recommandations du CERT-FR 2020 : https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/

[7] Durcissement et recommandations du CERT-FR 2021 : https://www.cert.ssi.gouv.fr/dur/CERTFR-2021-DUR-001/

[8] Rapport Microsoft concernant Hafnium : https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[9] Rapport Volexity : https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

[10] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004/

[11] Publication du chercheur Orange Tsai : https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell

[12] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-017/

[13] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-018/

[14] Avis CERT-FR : https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-267/

[15] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-007/

[16] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-001/

[17] Rapport FireEye : https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

[18] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-006/

[19] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-011/

[20] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-014/

[21] Alerte CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

[22] Guide d'hygiène informatique publié par l'ANSSI : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Version 1.0.4 - 22/02/2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr