Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC
GovCERT.ch

Cyber Security Update - Secteur de la Santé

À USAGE INTERNE UNIQUEMENT

Date : 8 juillet 2021
Version : v1.0
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distribution : Secteur de la Santé MELANI, H+, HIN

Actualités (Juin 2021)

La situation en matière de cybersécurité s'est légèrement détendue au cours du mois de juin :

- Vulnérabilité critique dans le service d'impression de Windows
- Nouvelle attaque par ransomware contre un hôpital
- Les acteurs des ransomwares changent leur mode opératoire
- Les acteurs du ransomware déconseillent l'utilisation de produits VPN connus

Le "Cyber Security Update" part en vacances d'été

En raison de la situation relativement détendue du COVID-19 et l'arrivée des vacances d'été, dont l'expérience a montré qu'elles entraînent une baisse significative des cyberattaques, GovCERT.ch a décidé d'envoyer le "Cyber Security Update" en vacances également. Par conséquent, **aucune publication n'est prévue pour les mois de juillet et d'août**. Le prochain numéro prévu sera publié à la fin du mois de septembre.

Bien entendu, nous restons à votre disposition à tout moment pendant les vacances d'été et continuons de suivre en permanence l'évolution de la menace. Nous nous réservons le droit de publier une mise à jour en cas de nécessité.

Vulnérabilité critique dans le service d'impression de Windows

Microsoft a publié le 8 juin un patch pour tous les systèmes d'exploitation Windows encore pris en charge, corrigeant une vulnérabilité dans le service de spouleur d'impression de Windows (CVE-2021-1675[1]). Selon les informations publiées initialement par Microsoft, un attaquant peut exploiter la vulnérabilité localement pour obtenir des droits d'administrateur non autorisés (élévation locale des privilèges – "Local Privilege Escalation"), justifiant ainsi sa classification comme risque "faible".

Le 21 juin 2021, Microsoft a mis à jour son évaluation de la criticité de la vulnérabilité de "faible" à "critique". Une analyse plus approfondie a montré que la vulnérabilité peut également être exploitée à distance pour accéder au système de la victime (exécution de code à distance – "Remote Code Execution" – RCE). Le 28 juin 2021, des chercheurs en sécurité ont également publié une preuve de concept ("Proof of Concept" – PoC) qui peut être utilisée pour exploiter la vulnérabilité à distance.

Des tests supplémentaires menés par des chercheurs en sécurité ont ensuite révélé que le correctif publié le 8 juin 2021 ne corrige que partiellement la vulnérabilité[2]. Ceci a été confirmé par Microsoft le 1er juillet[3]. Un nouveau patch a été publié le 7 juillet, ne couvrant pour l'instant que certains systèmes d'exploitation. **L'application du patch, respectivement des contre-mesures recommandées par Microsoft, doivent être mise en œuvre rapidement**.

Une nouvelle attaque par ransomware contre un hôpital

Les organismes de santé ont également été visés par des cyberattaques en juin 2021. Le "Humber River Hospital" de Toronto (Canada) a été attaqué mi-juin par des cybercriminels avec un ransomware inconnu. L'hôpital compte 772 lits et traite plus de 150'000 patients par an. Selon ses propres déclarations[4], tous les systèmes ont été temporairement arrêtés en réponse à l'attaque et les patients urgents ont été temporairement détournés.

Malheureusement, la famille de ransomware à l'origine de l'attaque demeure inconnue, tout comme des informations si / quel type de données ont été volé du réseau de l'hôpital.

Des acteurs de ransomware changent leur mode opératoire

Le mois de juin 2021 a vu deux acteurs du rançongiciel changer leur le modus operandi :

- **Babuk** : En juin, les auteurs du ransomware "Babuk" ont annoncé[5] l'arrêt du chiffrement des données et les systèmes de leurs victimes. Ces criminels veulent plutôt se concentrer sur le "kidnapping" de données d'entreprise à l'avenir, avec lesquelles ils feront chanter les victimes. Babuk a ainsi fait la une des journaux au printemps 2021

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675

[2] https://isc.sans.edu/forums/diary/CVE20211675+Incomplete+Patch+and+Leaked+RCE+Exploit/27588/

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

[4] https://www.hrh.ca/2021/06/15/code-grey/

[5] https://hotforsecurity.bitdefender.com/blog/babuk-ransomware-gang-says-its-no-longer-interested-in-encrypting-data-would-rather-kidnap-it-instead-25910.html

après que des organisations de police américaines se soient fait voler puis chiffrer des données.

- **REvil** : Fin juin 2021, des chercheurs en sécurité ont repéré des échantillons de logiciels malveillants ("malware") attribués au ransomware "REvil" (également connu sous le nom de "Sodinokibi"). Contrairement aux échantillons de malware précédemment lié à ce groupe, ceux-ci ne ciblent pas les systèmes basés sur Windows, mais les systèmes de stockage en réseau (NAS) et les systèmes virtuels (VMware ESXi)[6].

Les acteurs du ransomware déconseillent l'utilisation de certains produits VPN

Dans un tweet[7], les chercheurs en sécurité de "MalwareHunterTeam" ont déclaré que les acteurs du ransomware déconseillent l'utilisation de "Pulse Secure" et de "SonicWall VPN". Les deux produits ont présenté cette année des vulnérabilités critiques qui ont permis à des cybercriminels d'accéder à des réseaux d'entreprise et de les chiffrer à l'aide de ransomware. Il n'est pas clair quels acteurs du ransomware sont impliqués et d'où provient la citation. Nous pensons qu'elle provient très probablement d'une discussion entre les acteurs et une victime de ransomware.

Recommandations

- Les systèmes exposés à Internet tels que RDP, les services VPN, etc. doivent toujours être maintenus au dernier niveau de patch. **Les mises à jour de sécurité doivent être appliquées rapidement.**

- Les **accès à distance** tels que VPN et RDP ainsi que tous les autres accès aux ressources internes (par exemple webmail, Sharepoint, etc.) doivent être sécurisés par un second facteur (**authentification à deux facteurs** - 2FA). Assurez-vous que vous disposez des logs journalisant les tentatives d'accès réussies et échouées sur une période suffisamment longue. Stockez ces données de manière centralisée et évaluez-les régulièrement.

- Bloquer les adresses IP connues des serveurs de commande et contrôle (C&C) des botnets en mettant en œuvre le **flux MELANI BGP** (contact : outreach@govcert.ch). Vous pouvez vérifier si vous ou votre fournisseur mettez déjà en œuvre cette protection en tentant d'accéder aux adresses de test suivantes dans votre navigateur web. Si la connexion échoue, vous êtes déjà protégé :
  - http://ip-protection.govcert.ch
  - http://melbl-protection.govcert.ch

- Bloquer les noms de domaine connus des serveurs de commande et de contrôle (C&C) des botnets en mettant en œuvre la **RPZ MELANI** ou le **résolveur DNS sécurisé** (contact : outreach@govcert.ch)

- Bloquer la réception de **pièces jointes dangereuses** sur votre passerelle de messa-

[6] https://www.heise.de/news/Verschluesselungstrojaner-REvil-hat-es-nun-auf-virtuelle-Maschinen-abgesehen-6122156.html

[7] https://twitter.com/malwrhunterteam/status/1400339083596083201

gerie, y compris les **documents Office contenant des macros**. Une recommandation des extensions de fichiers à bloquer se trouve ici :
  - https://www.govcert.ch/downloads/blocked-filetypes.txt

- Créer **régulièrement des sauvegardes de vos données**. Utilisez le principe de génération (quotidien, hebdomadaire, mensuel - au moins 2 générations de chaque). Assurez-vous que vous **déconnectez physiquement** le support sur lequel vous avez créé la copie de sauvegarde de l'ordinateur ou du réseau après le processus de sauvegarde.

- Utilisez une liste telle que URLHaus[8] pour **empêcher** le téléchargement de **malware**.

- **Prenez au sérieux les notifications** des autorités concernant un problème de sécurité dans votre entreprise. En cas de doute sur l'authenticité d'un rapport, appelez l'autorité qui l'a envoyé.

- Veillez à ce que les **mises à jour de sécurité soient appliquées rapidement**. Les mises à jour de sécurité hautement critiques doivent être appliquées immédiatement et ne doivent pas être reportées à la prochaine fenêtre de maintenance.

Contact GovCERT

GovCERT est en tout temps à votre disposition, que ce soit en cas d'incident de sécurité avéré mais également en cas de soupçons (par exemple pour l'analyse d'emails suspects) :

Adresse email: incidents@govcert.ch
Permanence téléphonique : +41 79 152 20 80 (**uniquement en cas d'urgence !**)

Contactez outreach@govcert.ch en cas de questions techniques ou d'intérêt pour l'implémentation de services offerts par NCSC.

[8] https://urlhaus.abuse.ch/