C:YLLeNe

www.groupe-cyllene.com

Bulletin de sécurité

Edito

Et c'est un « essai » pour cette rentrée scolaire 2023 !

1ère mi-temps :
Elle est marquée par la Coupe du monde de rugby qui se déroule en France du 8 septembre au 28 octobre.
L'opportunité d'un tel évènement suscite forcément plus d'actes malveillants de cybercriminalité dont l'un des principaux vecteurs est l'hameçonnage ou le phishing.
Il nous faut donc redoubler de vigilance tant professionnelle que personnelle pour déjouer les pièges de ce genre d'attaque et vous invite à vous rappeler les bonnes pratiques présentées lors des séances de la sensibilisation Cyllene dont le 1er point est «Si un courriel vous semble douteux, ne cliquez pas sur les pièces jointes ou sur les liens».

Un rappel, Cyber@groupe-cyllene.com est l'adresse de contact privilégiée pour les demandes d'informations, les problèmes de sécurité, remontées d'incidents, mails suspects ...

2nd mi-temps :
Cette période estivale est l'occasion de faire un bilan de quelques évolutions dans l'équipe du « 15 » Cyber Cyllene. La team se renforce avec l'arrivée de Raphaël LEBLET (notre ailier : vitesse et agilité) en tant qu'Analyste Cybersécurité après 2 ans passé en temps qu'alternant Analyste SOC. Nous accueillons également Pierre CHEMIN (notre avant : perce les défenses) en tant qu'analyste SOC en alternance.

3ème mi-temps :
Toujours appréciée par les sportifs mais pas uniquement, ici elle se traduit par le projet de renforcement de nos certifications en la qualification SecNumCloud. Le match n'est pas gagné mais le processus est enclenché et notre dossier est en analyse à l'ANSSI... on va suivre la « transformation » !

L'actualité Cyber pour tous

- **Apple a corrigé l'exploit de type «zero-day» utilisé par le logiciel espion Pegasus avec iOS 16.6.1**

Jeudi, Apple a publié iOS 16.6.1, qui n'apporte pas de nouvelles fonctionnalités mais corrige des failles de sécurité, comme nous l'avions indiqué précédemment. Il est intéressant de noter que nous savons maintenant qu'iOS 16.6.1 corrige également un exploit utilisé par le logiciel espion Pegasus. Comme le rapporte TechCrunch, Citizen Lab - un groupe qui enquête sur les logiciels malveillants gouvernementaux - a découvert un exploit à zéro clic sur iOS qui permet aux attaquants de cibler les victimes avec le logiciel espion Pegasus de NSO Group. «La chaîne d'exploitation était capable de compromettre les iPhones utilisant la dernière version d'iOS (16.6) sans aucune interaction de la part de la victime», a écrit Citizen Lab dans un billet de blog. «Cette dernière découverte montre une fois de plus que la société civile est la cible d'exploits hautement sophistiqués et de logiciels espions mercenaires», explique Citizen Lab. Pour ceux qui ne le connaissent pas, Pegasus a été développé à l'intention des gouvernements et des organismes chargés de l'application de la loi. Le groupe NSO ne vend pas le logiciel espion aux utilisateurs ordinaires. Pourtant, la plupart des pays qui ont acheté Pegasus sont connus pour leurs violations des droits de l'homme, ce qui met en danger des personnes comme les journalistes et les opposants politiques.
L'article est consultable sur le site 9to5Mac.

- **Aviation : les cyberattaques passent par le WiFi**

Les terminaux avec WiFi des passagers offrent aux pirates un meilleur accès aux avions de ligne que l'avionique embarquée. À quelles compromissions de cybersécurité les avions de ligne sont-ils les plus exposés ? Tout dépend de la partie de leurs systèmes IT dont on parle. L'équipement avionique qui fait fonctionner l'aéronef est plutôt bien protégé contre le piratage, même s'il ne résiste pas à toutes les attaques. Par contre, les systèmes d'accès à Internet à bord des avions, qui connectent les passagers au web sont aussi vulnérables aux pirates que n'importe quel réseau au sol. Par rapport aux systèmes d'accès à Internet en vol, les systèmes avioniques en réseau sont plus difficiles à pirater. À cause en particulier de leur architecture (les réseaux avioniques ne sont pas connectés au web), aux fonctions limitées qu'ils exécutent et à leurs environnements d'exploitation généralement fermés. « Cependant, le piratage reste possible », comme l'a indiqué M. Kiley lui-même dans un document de recherche de Rapid7

de 2019 intitulé « Investigating CAN Bus Network Integrity in Avionics Systems ». Si l'on interroge des experts en cybersécurité sur les piratages connus d'avions commerciaux, il y a de fortes chances qu'ils citent en exemple le pirate informatique Chris Roberts. Selon un article paru en 2015 sur Wired.com, « Chris Roberts, chercheur en sécurité chez One World Labs, a déclaré à l'agent du FBI qui l'interrogeait en février de la même année, qu'il avait piraté le système de divertissement à bord (In-Flight Entertainment, IFE) d'un avion et écrasé le code de l'ordinateur de gestion de la poussée de l'avion alors qu'il se trouvait à bord du vol ».
Pour en savoir plus, nous vous invitons à lire l'article sur Le Monde Informatique.

- **Sous Windows 11, les accès SMB vont être protégés contre les attaques NTLM**

Microsoft continue de renforcer la sécurité de son système Windows 11 : cette fois-ci, l'entreprise américaine s'attaque à deux protocoles : NTLM et SMB. L'objectif est clair : réduire les risques d'attaques. Microsoft a dévoilé une nouvelle option de sécurité intégrée à Windows 11 Insider Preview (Build 25951) qui va permettre aux administrateurs d'empêcher le client SMB de Windows de tenter une connexion avec le protocole d'authentification NTLM : «Avec cette nouvelle option, un administrateur peut intentionnellement empêcher Windows de proposer NTLM via SMB.», peut-on lire dans l'article de Microsoft. Avec cette couche de sécurité supplémentaire qui empêche l'attaquant de récupérer le hash NTLM du compte de l'utilisateur (via une capture réseau, un serveur malveillant, etc.), Microsoft veut bloquer certaines attaques populaires comme pass-the-hash et NTLM relay, ainsi que les attaques brute force sur les hash NTLM. L'article est consultable sur le site IT-Connect.

Sécurité Technique

- **Vulnérabilité critique pour libwebp, en cours d'exploitation active - obtient le score CVSS maximum**

Google a attribué un nouvel identifiant CVE à une faille de sécurité critique dans la bibliothèque d'images libwebp pour le rendu d'images au format WebP, qui a fait l'objet d'une exploitation active dans la nature. Identifié sous le nom de CVE-2023-5129, elle a reçu la note de gravité maximale de 10.0 dans le système d'évaluation CVSS. Il a été décrit comme un problème lié à l'algorithme de codage Huffman. « Avec un fichier WebP sans perte spécialement conçu, libwebp peut écrire des données hors limites dans le tas. La fonction ReadHuffmanCodes() alloue le tampon HuffmanCode avec une taille qui provient d'un tableau de tailles précalculées : kTableSize. La valeur color_cache_bits définit la taille à utiliser. Le tableau kTableSize ne prend en compte que les tailles pour les tables de recherche de premier niveau de 8 bits, mais pas les tables de recherche de second niveau. libwebp autorise des codes allant jusqu'à 15 bits (MAX_ALLOWED_CODE_LENGTH). Lorsque BuildHuffmanTable() tente de remplir les tables de second niveau, il peut écrire des données hors limites. L'écriture OOB dans le tableau sous-dimensionné se produit dans ReplicateValue. ». Ce développement intervient après qu'Apple, Google et Mozilla ont publié des correctifs pour contenir un bogue - suivi séparément comme CVE-2023-41064 et CVE-2023-4863 - qui pourrait entraîner l'exécution d'un code arbitraire lors du traitement d'une image spécialement élaborée. Les deux failles sont soupçonnées de résoudre le même problème sous-jacent dans la bibliothèque. Selon le Citizen Lab, CVE-2023-41064 aurait été enchaîné avec 2023-41061 dans le cadre d'une chaîne d'exploitation iMessage sans clic nommée BLASTPASS pour déployer un logiciel espion mercenaire connu sous le nom de Pegasus. D'autres détails techniques sont actuellement inconnus. Mais la décision de considérer à tort la vulnérabilité CVE-2023-4863 comme une vulnérabilité de Google Chrome n'a pas tenu compte du fait qu'elle affecte également toutes les autres applications qui s'appuient sur la bibliothèque libwebp pour traiter les images WebP, ce qui indique qu'elle a un impact plus large que ce que l'on pensait auparavant. Une analyse réalisée par Rezillion la semaine dernière a révélé une liste d'applications, de bibliothèques de code, de cadres et de systèmes d'exploitation largement utilisés qui sont vulnérables à la vulnérabilité CVE-2023-4863. L'article est consultable sur le site TheHackerNews.

- **Publication d'un exploit pour la faille de contournement de l'authentification de Microsoft SharePoint Server**

Un code d'exploitation de démonstration a fait surface sur GitHub pour une vulnérabilité critique de contournement de l'authentification dans Microsoft SharePoint Server, permettant une escalade des privilèges. Répertoriée sous le nom de CVE-2023-29357, cette faille de sécurité peut permettre à des attaquants non authentifiés d'obtenir des privilèges d'administrateur à la suite d'une exploitation réussie dans le cadre d'attaques peu complexes qui ne nécessitent pas d'interaction de la part de l'utilisateur. «Un attaquant ayant accès à des jetons d'authentification JWT usurpés peut les utiliser pour exécuter une attaque réseau qui contourne l'authentification et lui permet d'accéder aux privilèges d'un utilisateur authentifié», a expliqué Microsoft en juin lorsqu'elle a corrigé la vulnérabilité. «Un attaquant qui réussirait à exploiter cette vulnérabilité pourrait obtenir des privilèges d'administrateur. L'attaquant n'a besoin d'aucun privilège et l'utilisateur n'a pas besoin d'effectuer une quelconque action». Une règle YARA est également disponible pour aider les défenseurs du réseau à analyser les journaux à la recherche de signes d'exploitation potentielle sur leurs serveurs SharePoint à l'aide de l'exploit CVE-2023-29357 PoC. Bien que l'exploit existant ne permette pas l'exécution immédiate de code à distance, il est fortement recommandé d'appliquer les correctifs de sécurité publiés par Microsoft au début de cette année, à titre de mesure préventive contre les attaques potentielles.
Pour en savoir plus, n'hésitez pas à consulter cet article depuis le site web Bleeping Computer.

- **Le CERT-FR décortique la cyberattaque contre le CHRU de Brest**

Six mois après la cyberattaque ayant frappé le CHRU de Brest, le CERT-FR est revenu sur le déroulé de l'incident et le mode opératoire d'un groupe de cybercriminels liés à FIN12. Le CHRU de Brest se souviendra longtemps du jeudi 9 mars. À 20h33, l'établissement de santé a en effet détecté une cyberattaque ayant impacté ses serveurs. Grâce à la réactivité des équipes en place prévenues par l'Anssi, le CHRU a pu éviter le pire, cette attaque ayant pu être bloquée avant d'aller à son terme. Six mois après cet incident, le CERT-FR - en accord avec le RSSI du CHRU de Brest Jean-Sylvain Chavanne - publie un rapport qui revient sur le déroulé de cet incident et le mode opératoire du cybergang FIN12 qui en est à l'origine. « Ce rapport de CTI démontre notamment l'importance d'avoir une double authentification et une politique de patch des vulnérabilités, surtout les plus classiques, pour éviter les élévations de privilèges », a fait savoir Jean-Sylvain Chavanne. « L'accès initial au système d'information a été effectué depuis un service de bureau à distance exposé et accessible sur Internet. Les opérateurs du MOA ont utilisé des authentifiants valides d'un professionnel de santé pour se connecter. Il est probable que les authentifiants du compte soient issus de la compromission par un information stealer du poste utilisateur, dans le cadre d'une campagne de distribution opportuniste », explique le CERT-FR. Les attaquants ont utilisé leur accès de bureau à distance afin d'exécuter deux portes dérobées : SystemBC et Cobalt Strike. Après avoir tenté d'exploiter les vulnérabilités LocalPotato, trois codes ont été employés pour essayer également de récupérer des données d'authentification : AccountRestore (bruteforce de comptes Active Directory), SharpRoast (attaque par kerberoasting) et Mimikatz (pour de l'extraction d'authentifiants en environnement Windows). Ces incidents présentent des caractéristiques techniques dont la plupart sont similaires à celles observées au CHU : accès initial au système d'information par l'utilisation d'authentifiants valides ; utilisation conjointe des codes malveillants SystemBC et Cobalt Strike ; le stockage de charges dans le répertoire C:\Users\Public\Music\ ; nom du chiffreur similaire : xxx.exe, bien que celui-ci n'ait pas pu être observé dans l'incident du CHU. Les attaquants ont employé deux portes dérobées : SystemBC et Cobalt Strike ». « D'après les analyses de l'Anssi, les attaquants responsables de l'incident du CHU de Brest pourraient donc être affiliés à différentes attaques par rançongiciel. Ils auraient utilisé les rançongiciels Ryuk, puis Conti, avant de distribuer Hive, Nokoyawa, Play et Royal. Une analyse historique de leur mode opératoire les lie à FIN12 ainsi qu'à d'autres opérations de rançongiciels ayant succédé à la fin des opérations du groupe Conti (Wizard Spider) ». L'article est consultable sur le site Le Monde Informatique.

Comprendre et Appliquer la protection des données

- **Données personnelles : la Cnil prépare un guide pour les « traitements critiques »**

La Cnil a lancé, le 28 août 2023, une consultation publique sur son projet de recommandation relatif à la « sécurité des traitements critiques » de données personnelles. Ce document unique concernera les bases de données « à caractère hautement personnel » concernant « une part importante de la population française ». Dans sa version actuelle, le texte recommande notamment aux organisations concernées la mise en place d'un CSIRT et d'une gouvernance dédiée à la protection des données. Elles devront par ailleurs réaliser un exercice de cybersécurité au moins une fois tous les 2 ans et une sauvegarde hors ligne chiffrée au moins une fois par an. Tout nouveau déploiement d'un traitement critique des données nécessitera une étude d'impact et un état des lieux des risques. Les organisations concernées devront enfin privilégier les outils open source et la logique « zero trust ». La consultation est ouverte aux organismes publics et privés jusqu'au 8 octobre 2023. La Cnil publiera la recommandation finalisée début 2024. L'article est consultable sur le site IN CYBER.