BULLETIN DE VEILLE N°07

ANPT-2023-BV-07

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic."
- Stephane Nappo -

Juillet 2023

Alertes de sécurité

Firefox 115

Firefox 115 corrige des vulnérabilités de haute sévérité de type "Use-After-Free"

05 Juillet 2023

Mozilla a annoncé la publication de Firefox 115 dans le canal stable avec des correctifs pour 12 vulnérabilités, y compris deux bogues de haute sévérité de type "use-after-free".

CVE-2023-37201, le premier des problèmes de haute sévérité est une faille dans la génération de certificats WebRTC.

Projet open source, WebRTC permet la communication en temps réel dans les navigateurs web et les applications mobiles, via des interfaces de programmation d'applications (API).

Un attaquant aurait pu déclencher une condition "use-after-free" lors de la création d'une connexion WebRTC via HTTPS.

La seconde vulnérabilité, CVE-2023-37202, est décrite comme un problème potentiel d'utilisation après la libération dû à une inadéquation des compartiments dans le moteur JavaScript et WebAssembly open source SpiderMonkey.

Le fabricant de navigateurs indique que la dernière mise à jour de Firefox corrige également des bogues de sécurité de la mémoire de haute sévérité qui auraient pu conduire à l'exécution d'un code arbitraire. Ces failles sont regroupées sous les noms de CVE-2023-37211 et CVE-2023-37212.

Firefox 115 comprend également des correctifs pour huit vulnérabilités de gravité moyenne qui conduisent à des sites malveillants plaçant des traceurs sans autorisation, à l'exécution de code arbitraire, à des attaques par usurpation, à l'usurpation d'URL, au téléchargement de fichiers contenant du code malveillant, à la condition "use-after-free", et au fait de tromper les utilisateurs pour qu'ils soumettent des données sensibles à des sites malveillants.

Mozilla a également annoncé que Firefox ESR 102.13 et Thunderbird 102.13 ont été publiés avec des correctifs pour cinq vulnérabilités, y compris les bogues de sécurité de mémoire et d'utilisation après la mort de haute gravité qui ont été corrigés dans Firefox 115.

Source : *https://bit.ly/4561j5v*

Chrome 115

Chrome 115 corrige 20 vulnérabilités

19 Juillet 2023

Google a annoncé la sortie de Chrome 115 dans le canal stable, avec des correctifs pour 20 vulnérabilités, dont 11 signalées par des chercheurs externes.

Parmi les failles de sécurité signalées par des chercheurs externes, quatre sont considérées comme très graves. D'après les primes aux bugs versées, les plus importantes sont CVE-2023-3727 et CVE-2023-3728, deux problèmes d'utilisation après la libération dans WebRTC. Google indique qu'il a versé une récompense de 7 000 dollars pour chacun d'entre eux.

La troisième faille de haute sévérité que Chrome 115 résout est un autre bug de type "use-after-free", cette fois-ci dans les groupes d'onglets. Repérée comme CVE-2023-3730, la vulnérabilité a été récompensée par une prime de 2 000 dollars.

Le quatrième problème de haute gravité, CVE-2023-3732, est décrit comme un accès mémoire hors limites dans Mojo. Le bogue a été découvert par Mark Brand, chercheur du Google Project Zero, et, conformément aux règles de Google, aucune prime ne sera versée pour ce bogue.

Chrome 115 résout six vulnérabilités de gravité moyenne signalées en externe, qui sont décrites comme des failles d'implémentation inappropriées dans les composants WebApp Installs, Picture In Picture, Web API Permission Prompts, Custom Tabs, Notifications et Autofill.

Cette version du navigateur résout également un bogue de faible gravité, à savoir une validation insuffisante des entrées non fiables dans les thèmes.

Le géant de l'internet ne mentionne pas que les vulnérabilités nouvellement résolues ont été exploitées dans le cadre d'attaques malveillantes.

Comme d'habitude, les détails techniques sur les vulnérabilités résolues sont gardés secrets jusqu'à ce que la dernière mise à jour de Chrome soit installée par la plupart des utilisateurs.

Source : https://bit.ly/3DvCjbX

Apple

Apple corrige une autre faille du noyau exploitée dans le cadre de l'opération Triangulation

24 Juillet 2023

Apple a publié d'importantes mises à jour de sécurité pour ses plateformes phares iOS, macOS et iPadOS.

Le fabricant de Cupertino a annoncé des correctifs pour des failles critiques d'exécution de code dans iOS et macOS, y compris un bug du noyau qui a été utilisé dans une chaîne d'exploitation documentée par Kaspersky.

Selon Apple, la faille du noyau (CVE-2023-38606) affecte à la fois les appareils fonctionnant sous iOS, iPadOS et macOS et a déjà été activement exploitée contre les versions d'iOS antérieures à iOS 15.7.1.

Au total, Apple a corrigé au moins 25 bogues de sécurité documentés qui hantent les iPhones et les iPads, y compris plusieurs problèmes qui exposent les appareils mobiles à des attaques par exécution de code. La mise à jour iOS 16.6 couvre également un bogue WebKit qui a été abordé pour la première fois dans le récent déploiement Rapid Security Response.

Apple a également corrigé des problèmes de sécurité dans son navigateur Safari (Safari 16.6), dans les anciennes versions des iPhones et iPads (iOS 15.7.8 et iPadOS 15.7.8) et dans macOS Ventura 13.5.

Source : https://bit.ly/43CCMUw

Adobe

Adobe publie de nouveaux correctifs pour les vulnérabilités exploitées de ColdFusion

17 Mai 2023

La société de cybersécurité Rapid7 a signalé des attaques visant des utilisateurs de ColdFusion. L'analyse a montré que les attaquants avaient exploité la CVE-2023-29298 et l'avaient enchaînée avec ce qui semblait être la CVE-2023-38203.
Rapid7 a souligné à l'époque que le correctif d'Adobe pour CVE-2023-29298 était incomplet et facile à contourner.
La CVE-2023-38203 a été signalée à Adobe par deux parties, dont des chercheurs de la société de sécurité open source ProjectDiscovery.
Le 12 juillet, ProjectDiscovery a publié une analyse de CVE-2023-29300, une vulnérabilité qui pourrait conduire à l'exécution de code à distance. Toutefois, cette analyse a également révélé par inadvertance la CVE-2023-38203 qui, à l'époque, n'avait pas encore été corrigée. Adobe a publié des correctifs le 14 juillet.
Le 19 juillet, la société a republié son billet de blog après qu'elle a constaté que le correctif d'Adobe pour CVE-2023-38203 était incomplet et que l'un des derniers correctifs ColdFusion, pour CVE-2023-38204, aborde en fait ce contournement du correctif.

Le mercredi 19 juillet, Adobe a annoncé une nouvelle mise à jour de ColdFusion pour corriger trois nouvelles CVE. L'une d'entre elles, CVE-2023-38205, est le contournement de CVE-2023-29298.
La CVE-2023-38205 a été exploitée dans la nature dans le cadre d'attaques limitées.
Si l'expression "attaques limitées" pourrait suggérer une exploitation par des acteurs de la menace parrainés par un État dans le cadre d'opérations très ciblées, les vulnérabilités de ColdFusion sont également connues pour être exploitées par des groupes de cybercriminels motivés par le profit.
Adobe a également publié un correctif pour CVE-2023-38206, une vulnérabilité ColdFusion découverte par le chercheur Brian Reilly, qui a récemment été crédité par Adobe d'une autre faille ColdFusion répertoriée sous le nom de CVE-2023-29301. Le calendrier suggère que CVE-2023-38206 a pu être attribué après que le correctif pour CVE-2023-29301 a été contourné.

Source : https://bit.ly/47bSB7r

Android

Les mises à jour de sécurité d'Android corrigent 3 vulnérabilités exploitées

06 Juillet 2023

Les mises à jour de sécurité que Google a publiées pour Android corrigent 43 vulnérabilités, dont trois ont été exploitées dans le cadre d'attaques.

Les failles exploitées, identifiées comme CVE-2023-2136, CVE-2023-26083 et CVE-2021-29256, ont un impact sur les composants System et Arm Mali d'Android.

La société indique qu'il y a des indications que ces défauts de sécurité peuvent faire l'objet d'une exploitation limitée et ciblée.

La CVE-2023-2136 a été divulguée en avril comme une vulnérabilité zero-day dans le navigateur Chrome, et est décrite comme un problème de débordement d'entier dans Skia.

Les appareils utilisant un niveau de correctif de sécurité 2023-07-01 ou plus récent sont protégés contre cette vulnérabilité et 22 autres défauts de sécurité dans les composants Framework et System de la plateforme, y compris un problème d'exécution de code à distance de gravité critique répertorié sous le nom de CVE-2023-21250.

Les deux bogues Arm exploités ont été corrigés dans le cadre du niveau de correctif de sécurité 2023-07-05 d'Android, qui résout un total de 20 failles dans les composants Kernel, Arm, Imagination Technologies, MediaTek et Qualcomm.

La première des vulnérabilités, CVE-2021-29256, est une vulnérabilité d'escalade de privilèges affectant les pilotes Midgard, Bifrost et Valhall Mali du noyau.

Le second problème exploité, CVE-2023-26083, est décrit comme une vulnérabilité de fuite de mémoire dans les pilotes de noyau Midgard, Bifrost, Valhall, et 5th gen Mali GPU.

Google a également annoncé des mises à jour de sécurité pour les appareils Pixel, afin de corriger 14 vulnérabilités dans les composants Kernel, Pixel et Qualcomm. Deux des failles, conduisant à une élévation des privilèges et à un déni de service.

Source : https://bit.ly/474oqPF

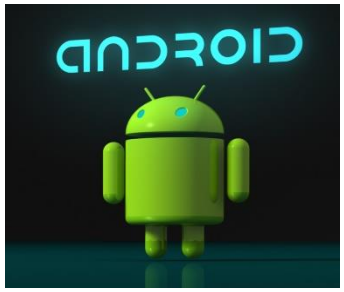
Actualité

CherryBlos, un nouveau logiciel malveillant pour Android, utilise l'OCR pour voler des données sensibles

Une nouvelle souche de malware Android appelée CherryBlos a été observée en train d'utiliser des techniques de reconnaissance optique de caractères (OCR) pour collecter des données sensibles stockées dans des images.

CherryBlos est distribué via de faux messages sur les plateformes de médias sociaux et est doté de capacités permettant de voler des informations d'identification liées à des portefeuilles de crypto-monnaies et d'agir comme un clipper pour substituer des adresses de portefeuilles lorsqu'une victime copie une chaîne correspondant à un format prédéfini dans le presse-papiers.

Une fois installée, l'application demande aux utilisateurs de lui accorder des autorisations d'accès, ce qui lui permet de s'octroyer automatiquement des autorisations supplémentaires en fonction des besoins. Comme mesure de défense, les utilisateurs qui tentent de désinstaller l'application en entrant dans l'application Paramètres sont redirigés vers l'écran d'accueil.



CherryBlos utilise la reconnaissance optique de caractères pour reconnaître des phrases mnémoniques potentielles à partir d'images et de photos stockées sur l'appareil, dont les résultats sont périodiquement téléchargés vers un serveur distant.

Une autre application développée par les acteurs de la menace CherryBlos, nommée Synthnet,a été trouvé sur le Google Play Store, mais sans le programme malveillant intégré. L'application, nommée Synthnet, a depuis été supprimée par Google.

La plupart des applications ont été téléchargées sur le Play Store en 2021 et ciblent les utilisateurs d'Android.

L'année dernière, Google a commencé à prendre des mesures pour limiter l'utilisation abusive des API d'accessibilité par des applications Android malveillantes afin de recueillir secrètement des informations sur des appareils compromis, en bloquant complètement l'utilisation des fonctions d'accessibilité par les applications chargées latéralement.

Mais les voleurs et les tondeuses ne représentent qu'un des nombreux types de logiciels malveillants qui sont utilisés pour suivre des cibles et recueillir des informations intéressantes, ce qui constitue une grave menace pour la vie privée et la sécurité des personnes.

Une nouvelle recherche a révélé qu'une application de surveillance appelée SpyHide recueille furtivement les données téléphoniques privées de près de 60 000 appareils Android dans le monde depuis au moins 2016.

"Certains des opérateurs ont plusieurs appareils connectés à leur compte, certains ayant jusqu'à 30 appareils qu'ils ont surveillés pendant plusieurs années, espionnant tout le monde dans leur vie", a déclaré un chercheur en sécurité, qui se fait appeler maia arson crimew.

Il est donc essentiel que les utilisateurs restent vigilants lorsqu'ils téléchargent des applications provenant de sources non vérifiées, qu'ils vérifient les informations sur les développeurs et qu'ils examinent attentivement les commentaires sur les applications afin de limiter les risques potentiels.

Le fait que rien n'empêche les acteurs de la menace de créer de faux comptes de développeurs sur le Play Store pour distribuer des logiciels malveillants n'est pas passé inaperçu chez Google.

Le géant de la recherche a annoncé qu'il exigerait de tous les nouveaux comptes de développeurs s'enregistrant en tant qu'organisation qu'ils fournissent un numéro D-U-N-S valide attribué par Dun & Bradstreet avant de soumettre des applications, dans le but de renforcer la confiance des utilisateurs. Ce changement entrera en vigueur le 31 août 2023.

Source : *https://bit.ly/458jYxI*

TeamTNT vole les informations d'identification d'Azure et de Google Cloud

Une nouvelle campagne de vol d'informations d'identification a été découverte, ciblant les services Azure et Google Cloud Platform (GCP). Cette campagne présente des similitudes avec le groupe de cryptojacking TeamTNT.

Les attaques en cours ciblent spécifiquement les instances Docker orientées vers le public, en déployant un module de propagation qui ressemble à un ver. Ces attaques font partie d'un ensemble d'intrusions plus large qui s'est précédemment concentré sur les ordinateurs portables Jupyter en décembre 2022.

Entre le 15 juin 2023 et le 11 juillet 2023, les chercheurs ont découvert jusqu'à huit nouvelles versions du script de collecte d'informations d'identification, ce qui témoigne d'une campagne en constante évolution.

Les dernières itérations du malware ont été conçues pour collecter des informations d'identification à partir de diverses sources, notamment AWS, Azure, Google Cloud Platform, Censys, Docker, Filezilla, Git, Grafana, Kubernetes, Linux, Ngrok, PostgreSQL, Redis, S3QL et SMB.

Les méthodes utilisées pour collecter les informations d'identification et les fichiers ciblés présentent des similitudes avec une précédente campagne de ciblage de Kubelet menée par TeamTNT en septembre 2022.

En outre, ces attaques s'alignent sur une campagne en cours de TeamTNT connue sous le nom de Silentbob, qui exploite des services cloud mal configurés pour distribuer des logiciels malveillants dans le cadre d'une initiative de test.

Toutefois, les experts soupçonnent également un lien avec SCARLETEEL en raison de la similitude de l'infrastructure

d'attaque. Le fait que la campagne SCARLETEEL 2.0 ait impliqué un mineur de crypto-monnaie utilisant la même adresse de portefeuille Monero constitue un élément de preuve important permettant de relier ces campagnes.
Cela suggère un lien étroit entre les campagnes. Cependant, il est reconnu qu'il est difficile d'attribuer définitivement ces activités à TeamTNT en raison des variations dans les TTP, malgré l'existence d'une infrastructure commune.
Cette campagne met en évidence la croissance d'un acteur expérimenté dans le domaine de l'informatique dématérialisée, qui possède des connaissances sur plusieurs technologies. Si AWS est traditionnellement une cible de choix pour ce type d'acteurs, l'inclusion d'identifiants Azure et GCP laisse entrevoir d'autres sources de données précieuses. Restreindre l'accès à Docker en fonction des besoins de l'organisation et minimiser l'exposition aux connexions externes contribuera à réduire les risques.

Source : *https://bit.ly/3YhTK9x*

Des milliers d'identifiants OpenAI volés pour être vendus sur le Dark Web

Les acteurs de la menace montrent un intérêt croissant pour les outils d'intelligence artificielle générative, avec des centaines de milliers d'identifiants OpenAI en vente sur le Dark Web et l'accès à une alternative malveillante pour ChatGPT.
Les cybercriminels, qu'ils soient moins expérimentés ou chevronnés, peuvent utiliser ces outils pour créer des courriels d'hameçonnage plus convaincants, adaptés au public visé, afin d'augmenter les chances de réussite de l'attaque.
En six mois, les utilisateurs du Dark Web et de Telegram ont mentionné ChatGPT, le chatbot d'intelligence artificielle d'OpenAI, plus de 27 000 fois, selon les données de Flare, une société de gestion de l'exposition aux menaces.
En analysant les forums et les places de marché du Dark Web, les chercheurs de Flare ont remarqué que les identifiants d'OpenAI font partie des dernières marchandises disponibles.
Les chercheurs ont identifié plus de 200 000 identifiants OpenAI en vente sur le Dark Web sous la forme de logs de voleurs.

Un rapport publié en juin par l'entreprise de cybersécurité Group-IB indique que les marchés illicites du Dark Web ont échangé des journaux de logiciels malveillants de vol d'informations contenant plus de 100 000 comptes ChatGPT.
L'intérêt des cybercriminels pour ces utilitaires est tel que l'un d'entre eux a développé un clone de ChatGPT appelé WormGPT et l'a entraîné sur des données axées sur les logiciels malveillants.
L'outil est présenté comme "la meilleure alternative GPT pour les blackhats" et une alternative ChatGPT "qui vous permet de faire toutes sortes de choses illégales".
WormGPT s'appuie sur le modèle de langage large open-source GPT-J développé en 2021 pour produire des textes de type humain. Son concepteur indique qu'il a entraîné l'outil sur un ensemble varié de données, en mettant l'accent sur les données relatives aux logiciels malveillants, mais il n'a fourni aucune indication sur les ensembles de données spécifiques.
Le fournisseur de solutions de sécurité pour les courriels SlashNext a pu accéder à WormGPT et a effectué quelques tests pour déterminer le danger potentiel qu'il représente.
Les chercheurs se sont concentrés sur la création de messages adaptés aux attaques de type "business email compromise" (BEC).
Bien qu'il soit difficile de se défendre contre cette menace émergente, les entreprises peuvent s'y préparer en formant leurs employés à la vérification des messages réclamant une attention urgente, en particulier lorsqu'ils comportent un élément financier.
L'amélioration des processus de vérification des courriels devrait également porter ses fruits, avec des alertes pour les messages provenant de l'extérieur de l'organisation ou en signalant des mots-clés typiquement associés à une attaque BEC.

Source : *https://bit.ly/43MR4Sz*

Bon à savoir

Global Ransomware Onslaught: : Le GRIT découvre 14 nouveaux groupes de ransomwares

Dans le paysage en constante évolution des cybermenaces, les ransomwares restent des adversaires persistants et menaçants, causant des ravages chez les particuliers, les organisations et les gouvernements. L'équipe de recherche et de renseignement de GuidePoint (GRIT) a publié son rapport sur les ransomwares pour le deuxième trimestre 2023, qui fait état de statistiques choquantes :

- Le GRIT a surveillé un total de 1 177 victimes de ransomware signalées publiquement, qui ont été revendiquées par 41 groupes de menaces distincts. Ces chiffres indiquent une augmentation significative de 38 % des victimes de ransomware signalées publiquement par rapport au trimestre précédent et une augmentation stupéfiante de 100 % par rapport à la même période de l'année précédente (T2 2022).
- Notamment, les secteurs de la fabrication et de la technologie restent les plus touchés, représentant respectivement 14% et 11% des industries impactées, une tendance qui persiste depuis les observations du GRIT en 2022 et au 1er trimestre 2023.
- Au cours du trimestre, le secteur du conseil a connu une croissance relative inquiétante de 236 % des attaques de ransomware observées, suivi de près par le secteur de l'assurance avec une croissance relative de 160 %.

- Le rapport fait également état d'une recrudescence de l'activité des groupes de Ransomware-as-a-Service (RaaS) tout au long du trimestre, attribuée à l'émergence de 14 nouveaux groupes. Cela représente une augmentation substantielle de 260 % des groupes "First Seen" par rapport au premier trimestre.
- Dans le paysage RaaS, LockBit a occupé une position dominante dans les cinq secteurs les plus touchés, à l'exception du secteur de la santé, où il a été concurrencé par BianLian et Karakurt.

Les statistiques du deuxième trimestre 2023 soulignent une fois de plus l'escalade de la menace des ransomwares à laquelle les organisations du monde entier sont confrontées, émanant à la fois de gangs de ransomwares bien établis et de groupes opportunistes émergents.
Les chercheurs ont souligné que la réduction des barrières à l'entrée facilitée par les économies des logiciels criminels en tant que service et RaaS est susceptible d'attirer davantage d'acteurs malveillants à l'avenir.
Si les défenseurs bien préparés et disposant de ressources suffisantes peuvent avoir un avantage dans la lutte contre les logiciels malveillants et les rançongiciels historiques, les organisations plus petites ou disposant de moins de ressources sont exposées à des risques accrus en raison de la montée en flèche du volume des menaces.
Le paysage des ransomwares, en constante évolution, comprend divers éléments, tels que des ransomwares recyclés, des logiciels criminels, et un accent mis sur l'extorsion de données, entre autres tactiques. L'échange d'informations entre la communauté de la sécurité et les forces de l'ordre joue un rôle crucial dans l'identification et la neutralisation de l'impact des groupes de ransomwares. Les efforts visant à améliorer l'échange de renseignements sur les menaces par le biais de collaborations publiques et privées restent une priorité absolue pour les organisations.

Source : *https://bit.ly/478Smdw*

Evènements

Evènement du mois

Un guide Digital Eagles sur la sécurité numérique - fraude et escroqueries

31 Juillet 2023

Online

https://bit.ly/3Kmek2M

Digital Eagles
Digital Eagle Events

L'utilisation de la technologie a facilité la vie à bien des égards, mais elle a également permis aux criminels de s'emparer plus facilement les informations personnelles. C'est pourquoi les utilisateurs doivent savoir comment les cybercriminels fonctionnent et comment se protéger de leurs tactiques afin de se sentir en confiance en ligne.

La session a été déroulé sur Microsoft Teams gratuitement. Une participation à une session d'équipes a été organisé par l'équipe Barclays Digital Eagles.

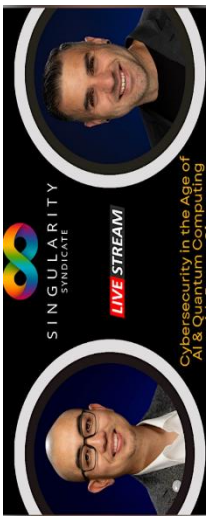
Evènement à venir

La cybersécurité à l'ère de l'IA et de l'informatique quantique

12 Août 2023

Online

https://bit.ly/3KmftHz



Il s'agit d'une excellente occasion d'en savoir plus sur l'avenir de la cybersécurité et sur la manière de protection contre les menaces les plus récentes.

Découvrez le rôle de l'IA dans la cybersécurité avec le professeur Danny, et comment se protéger des cyberattaques alimentées par l'IA.

Cette formation aborde aussi une introduction à l'informatique quantique et comment pourrait-elle influer sur le domaine de la cybersécurité, et ce qui pourrait être fait pour se préparer à l'avenir.

Référence	ANPT-2023-BV-07
Titre	Bulletin de veille N°07
Date de version	31 Juillet 2023
Contact	ssi@anpt.dz