BULLETIN DE VEILLE N°09

ANPT-2023-BV-09

"In the world of cyber security, the last thing you want is to have a target painted on you"
-- Tim Cook --

Septembre 2023

Alertes de sécurité

Apple

Les mises à jour d'urgence d'Apple corrigent trois nouvelles failles exploitées dans des attaques

21 Août 2023

Apple a publié des mises à jour de sécurité d'urgence pour corriger trois vulnérabilités "zero-day" qui ont été activement exploitées dans des attaques visant les utilisateurs d'iPhone et de Mac. Cela porte à 16 le nombre total de vulnérabilités "zero-day" corrigées par Apple cette année. Les vulnérabilités touchent différents composants des logiciels et appareils Apple, notamment le moteur de navigation WebKit, le cadre de sécurité et le cadre du noyau. L'exploitation de ces vulnérabilités pourrait permettre aux attaquants de contourner la validation des signatures, d'exécuter un code arbitraire par le biais de pages web malveillantes et d'élever les privilèges sur les systèmes locaux.

Apple a publié des mises à jour pour corriger ces vulnérabilités dans diverses versions logicielles, telles que macOS 12.7/13.6, iOS 16.7/17.0.1, iPadOS 16.7/17.0.1 et watchOS 9.6.3/10.0.1. Apple a notamment reconnu que l'une des vulnérabilités pouvait avoir été activement exploitée dans les versions d'iOS antérieures à iOS 16.7.

Les appareils concernés sont l'iPhone 8 et les versions ultérieures, l'iPad mini de 5e génération et les versions ultérieures, les Macs fonctionnant sous macOS Monterey et les versions ultérieures, et l'Apple Watch Series 4 et les versions ultérieures.

Les chercheurs en sécurité Bill Marczak du Citizen Lab de la Munk School de l'Université de Toronto et Maddie Stone du Threat Analysis Group de Google ont découvert et signalé les trois vulnérabilités zero-day. Ces chercheurs ont l'habitude de divulguer des vulnérabilités "zero-day" utilisées dans des attaques ciblées de logiciels espions contre des personnes à haut risque, telles que des journalistes, des politiciens de l'opposition et des dissidents.

En outre, Apple a récemment corrigé deux autres vulnérabilités de type "zero-day" (CVE-2023-41061 et CVE-2023-41064) dans le cadre d'une chaîne d'exploitation de type "zero-click" connue sous le nom de BLASTPASS, qui a été utilisée pour infecter des iPhones entièrement corrigés avec le logiciel espion commercial Pegasus de NSO Group.

Tout au long de l'année, Apple a activement corrigé les vulnérabilités de type "zero-day" afin de renforcer la sécurité de ses produits. Cela souligne l'importance de maintenir les logiciels et les appareils à jour pour se protéger contre les risques de sécurité connus.

Source : *https://bit.ly/3EVE2rY*

GitLab

GitLab publie des correctifs de sécurité urgents pour remédier à une faille critique

23 Août 2023

GitLab a publié des correctifs de sécurité critiques pour corriger une vulnérabilité, CVE-2023-5009, avec un score CVSS de 9.6. Cette vulnérabilité affecte toutes les versions de GitLab Enterprise Edition (EE) de 13.12 à 16.2.7, ainsi que de 16.3 à 16.3.4.

La vulnérabilité permet à un attaquant d'exécuter des pipelines en tant qu'autre utilisateur, en particulier via des politiques d'analyse de sécurité planifiées. Ceci est considéré comme un contournement d'une vulnérabilité précédemment corrigée, CVE-2023-3932.

L'exploitation de CVE-2023-5009 peut avoir de graves conséquences, notamment l'accès non autorisé à des informations sensibles, l'utilisation abusive des privilèges d'un utilisateur usurpé pour modifier le code source, ou l'exécution de code arbitraire sur le système.

C'est au chercheur en sécurité Johan Carlsson (joaxcar) que l'on doit la découverte et le signalement de cette vulnérabilité, que GitLab a rapidement corrigée dans les versions 16.3.4 et 16.2.7.

Il est essentiel que les utilisateurs de GitLab mettent rapidement à jour leurs installations vers la dernière version afin de limiter les risques potentiels. En outre, cette divulgation rappelle qu'un autre bogue critique de GitLab (CVE-2021-22205, CVSS score : 10.0) datant d'il y a deux ans est toujours activement exploité par des acteurs menaçants dans des attaques réelles, ce qui souligne l'importance de rester vigilant en ce qui concerne la sécurité des logiciels.

Source : *https://bit.ly/3tc32bH*

Google

Chrome : Google publie un correctif pour une faille Zero-Day activement exploitée

23 Août 2023

Google a réagi rapidement pour corriger une vulnérabilité zero-day dans le navigateur Chrome, connue sous le nom de CVE-2023-5217. Cette vulnérabilité sérieuse est due à un débordement de mémoire tampon basé sur le tas dans le format de compression VP8 de la bibliothèque libvpx, développée par Google et l'Alliance for Open Media (AOMedia). L'exploitation de cette faille peut entraîner des plantages de programme ou l'exécution de code malveillant, compromettant la disponibilité et l'intégrité du logiciel.

La découverte de la vulnérabilité est attribuée à Clément Lecigne du Threat Analysis Group (TAG) de Google, qui l'a signalée le 25 septembre 2023. Il a été noté que des logiciels espions commerciaux ont abusé de cette vulnérabilité pour cibler des individus à haut risque. Google n'a cependant pas divulgué de détails supplémentaires, si ce n'est qu'un exploit pour CVE-2023-5217 est en circulation.

Cette découverte porte à cinq le nombre de vulnérabilités zero-day corrigées dans Google Chrome cette année. Il est également suspecté que le fabricant de logiciels espions israélien Cytrox ait exploité une vulnérabilité de Chrome récemment corrigée (CVE-2023-4762) comme zero-day pour déployer une menace appelée Predator, bien que peu d'informations soient disponibles à ce sujet.

En réponse, Google a attribué un nouvel identifiant CVE, CVE-2023-5129, à une faille critique dans la bibliothèque d'images libwebp, précédemment identifiée sous CVE-2023-4863, en raison de son exploitation active.

Pour se protéger contre ces menaces potentielles, il est fortement recommandé aux utilisateurs de mettre à jour Chrome vers la version 117.0.5938.132, disponible pour Windows, macOS et Linux. Les utilisateurs de navigateurs basés sur Chromium, comme Microsoft Edge, Brave, Opera et Vivaldi, sont également invités à appliquer rapidement les correctifs disponibles.

Mozilla a également pris des mesures en publiant des mises à jour de Firefox pour résoudre la CVE-2023-5217, référencée à la gestion d'un flux multimédia VP8 contrôlé par un attaquant pouvant entraîner un débordement de mémoire tampon dans le processus de contenu. Ces mises à jour sont disponibles sous différentes versions de Firefox pour Android et ordinateurs.

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

Firefox

Firefox 118 corrige des vulnérabilités de haute gravité

25 Août 2023

Mozilla a récemment publié des mises à jour de sécurité pour Firefox et Thunderbird, corrigeant un total de neuf vulnérabilités dans leurs produits, dont certaines sont considérées comme des problèmes de haute gravité.

La version 118 de Firefox a été publiée dans le canal stable et comprend des correctifs pour les neuf vulnérabilités. Ces vulnérabilités concernent principalement des problèmes de mémoire, dont beaucoup peuvent conduire à des plantages exploitables.

Deux failles de haute sévérité, identifiées comme CVE-2023-5168 et CVE-2023-5169, sont identifiées comme des problèmes d'écriture hors limites dans les composants FilterNodeD2D1 et PathOps du navigateur. Mozilla a noté que ces deux problèmes pourraient entraîner un "plantage potentiellement exploitable dans un processus privilégié".

Une autre vulnérabilité de haute gravité, CVE-2023-5170, implique un problème de fuite de mémoire qui, s'il est exploité avec les données correctes, pourrait potentiellement conduire à une évasion du bac à sable.

Une condition "use-after-free" dans le compilateur Ion, répertoriée comme CVE-2023-5171, a également été corrigée. Cette faille permettait à un attaquant d'écrire deux octets NUL, causant un crash potentiellement exploitable.

Firefox 118 corrige également la CVE-2023-5172, un problème de corruption de mémoire dans Ion Hints qui pourrait conduire à une condition d'utilisation après la mort et à un plantage potentiellement exploitable.

En outre, cette mise à jour du navigateur résout plusieurs bogues de sécurité de la mémoire de haute sévérité suivis collectivement comme CVE-2023-5176. Mozilla indique qu'avec un effort suffisant, un attaquant pourrait potentiellement exploiter certaines de ces failles pour exécuter un code arbitraire.

La version 118 de Firefox inclut également des correctifs pour trois autres problèmes de gravité moyenne et faible liés à des bogues de mémoire.

Mozilla a également publié Firefox ESR 115.3 et Thunderbird 115.3, chacun avec des correctifs pour cinq vulnérabilités. Ces mises à jour incluent quatre des failles de haute sévérité corrigées dans Firefox 118, ainsi qu'un bogue de sévérité moyenne.

Mozilla n'a signalé aucun cas d'exploitation de ces vulnérabilités dans le cadre d'attaques malveillantes. Pour plus de détails, vous pouvez consulter la page des avis de sécurité de Mozilla.

Source : *https://bit.ly/48ybz9b*

Actualité

Des chercheurs en IA de Microsoft divulguent 38 To de données privées

Microsoft a exposé par accident une quantité importante de données internes sensibles, datant de plus de trois ans, par l'intermédiaire d'un dépôt GitHub public. La découverte a été faite par l'entreprise de sécurité informatique Wiz, qui a trouvé le dépôt GitHub nommé "robust-models-transfer", appartenant à la division de recherche en IA de Microsoft. Alors que le dépôt était censé donner accès à du code source ouvert et à des modèles d'IA pour la reconnaissance d'images, l'URL d'Azure Storage était mal configurée, accordant des permissions sur l'ensemble du compte.

L'analyse de Wiz a révélé que le compte contenait 38 To de données supplémentaires, y compris des sauvegardes d'ordinateurs personnels d'employés de Microsoft. Ces sauvegardes contenaient des informations sensibles telles que des mots de passe pour les services Microsoft, des clés secrètes et plus de 30 000 messages internes Microsoft Teams de 359 employés. En outre, le jeton mal configuré permettait non seulement de visualiser, mais aussi de supprimer et d'écraser des fichiers dans le compte de stockage.

Le problème provient de l'utilisation par Microsoft d'un jeton SAS (Shared Access Signature), qui est une URL signée permettant aux utilisateurs d'accéder aux données d'Azure Storage avec des autorisations et des dates d'expiration personnalisables. Le jeton SAS en question a été déposé pour la première fois sur GitHub en juillet 2020, et sa date d'expiration a été mise à jour 30 ans plus tard, en octobre 2021.

Microsoft a invalidé le jeton et l'a remplacé après que Wiz a signalé l'incident. Microsoft a précisé qu'aucune donnée client n'a été exposée et qu'aucun autre service interne n'a été mis en danger par ce problème. Cependant, Wiz a averti que les jetons SAS représentent un risque permanent pour la sécurité en raison d'un manque de surveillance et de gouvernance. Il recommande de limiter l'utilisation de ces jetons et souligne l'importance d'éviter les jetons SAS de compte pour le partage externe.

Source : *https://bit.ly/48ybAKh*

Après Microsoft et X, des hackers lancent une attaque DDoS sur Telegram

Le groupe pirate Anonymous Sudan a lancé une attaque par déni de service distribué (DDoS) contre la plateforme de messagerie Telegram en réponse à la suspension de leur compte principal par Telegram. Ces représailles ont été signalées par la société de renseignement sur les menaces SOCRadar.

Anonymous Sudan, qui affirme être motivé par des causes politiques et religieuses, a été impliqué dans diverses attaques DDoS visant des organisations dans de nombreux pays, dont l'Allemagne, l'Australie, le Danemark, la France, l'Inde, Israël, la Suède et le Royaume-Uni. Le groupe est apparu au début de l'année et a d'abord ciblé des sites web suédois.

En juin, Anonymous Sudan s'est fait connaître en lançant des attaques DDoS perturbatrices contre les services Microsoft 365, touchant Outlook, Microsoft Teams, OneDrive for Business, SharePoint Online et même la plateforme de cloud computing Azure de Microsoft. Microsoft a confirmé que ces attaques étaient à l'origine des perturbations.

En août, le groupe a ciblé X (anciennement Twitter) dans une attaque DDoS visant à faire pression sur Elon Musk pour qu'il lance le service Starlink au Soudan.

La récente attaque contre Telegram avait un motif différent des intérêts habituels du groupe et n'a pas atteint son objectif. En conséquence, les hacktivistes ont déplacé leur canal principal sur Telegram.

La raison exacte de l'interdiction du groupe par Telegram n'est pas claire, mais SOCRadar suppose qu'elle pourrait être liée à l'utilisation de comptes robots ou à la récente attaque sur X.

Il convient de noter que le groupe Anonymous Sudan qui mène des attaques DDoS et des dégradations n'est peut-être pas basé au Soudan et pourrait avoir des liens avec le groupe de pirates russes KillNet, selon les rapports de SOCRadar et Truesec. Les campagnes du groupe ne semblent pas être liées à des questions politiques soudanaises, elles ne cherchent pas à obtenir le soutien de groupes pro-islamiques et elles communiquent principalement avec des pirates russes, utilisant l'anglais et le russe au lieu de l'arabe. En outre, ils semblent distincts des hacktivistes soudanais d'Anonymous qui ont émergé au Soudan en 2019 et du mouvement mondial d'Anonymous.

Source : *https://bit.ly/3tcu3fk*

Des milliers de sites web populaires divulguent leurs secrets

La société Truffle Security, spécialisée dans la sécurité du code, a lancé un avertissement concernant la fuite d'informations sensibles, notamment d'informations d'identification, sur des milliers de domaines figurant dans la liste Alexa des 1 millions de sites web les plus fréquentés. Selon Truffle Security, environ 4 500 des sites web examinés ont exposé leur répertoire « .git ».

Un répertoire « .git » est créé lors de l'initialisation d'un dépôt Git et contient toutes les informations nécessaires à un projet, telles que les validations de code, les chemins d'accès aux fichiers, les données de contrôle de version, etc. Dans certains cas, ce répertoire peut contenir l'intégralité d'un code source privé, des fichiers de configuration, l'historique des livraisons et les identifiants d'accès.

Cette exposition des répertoires « .git » pourrait potentiellement fournir aux attaquants un accès au code source et aux

identifiants, leur permettant de lancer des attaques contre les applications web de la victime ou de rechercher des identifiants en direct pour des services tiers tels qu'AWS.

L'analyse des informations d'identification exposées a révélé que les clés AWS et GitHub étaient les secrets les plus fréquemment divulgués, représentant 45 % de toutes les informations d'identification. Truffle Security explique que les jetons GitHub sont souvent stockés dans le fichier de configuration Git lors du clonage du dépôt à distance, ce qui peut expliquer le nombre élevé de clés GitHub exposées.

Le rapport note également que les services tiers de marketing par courriel, tels que Mailgun, SendInBlue, Mailchimp et Sendgrid, représentent un pourcentage important des clés divulguées.

En ce qui concerne les identifiants GitHub exposés, Truffle Security a constaté qu'environ 67 % d'entre eux avaient des privilèges de niveau administrateur, et que tous avaient des autorisations de dépôt, ce qui permettait aux attaquants de prendre diverses mesures, y compris l'implantation potentielle de logiciels malveillants dans le code.

Une analyse plus poussée a révélé l'exposition d'une clé RSA privée correspondant au certificat TLS d'un domaine, permettant potentiellement des attaques de type "man-in-the-middle".

Truffle Security a tenté de contacter tous les propriétaires de sites concernés après avoir identifié et vérifié les secrets exposés, mais tous n'ont pas répondu.

L'entreprise reconnaît que ses recherches n'avaient qu'une portée limitée et qu'il existe potentiellement beaucoup d'autres sites web présentant des problèmes similaires. Les développeurs sont invités à faire preuve de prudence et à éviter d'exposer les répertoires « .git » en dehors du répertoire racine du site web afin de minimiser ces risques.

Source : *https://bit.ly/3PEC4RD*

Une nouvelle opération de cryptojacking cible des services AWS peu courants

Une opération de cryptojacking cloud-native connue sous le nom d'AMBERSQUID est apparue, se concentrant sur des offres Amazon Web Services (AWS) moins courantes comme AWS Amplify, AWS Fargate et Amazon SageMaker pour le minage illicite de crypto-monnaies. Sysdig, une société spécialisée dans la sécurité du cloud et des conteneurs, a découvert cette activité malveillante.

Principaux éléments de l'opération de cryptojacking AMBERSQUID :

AMBERSQUID cible les services AWS sans déclencher d'exigences d'approbation des ressources.
Il exploite plusieurs services AWS, ce qui complique la réponse aux incidents.
Sysdig a identifié la campagne en analysant les images Docker Hub et l'attribue avec une confiance modérée à des attaquants indonésiens sur la base de l'utilisation de la langue dans les scripts et les noms d'utilisateur.
Les attaquants utilisent les images Docker pour exécuter des mineurs de crypto-monnaie ou des scripts shell ciblant les services AWS.
AWS CodeCommit est utilisé de manière abusive pour créer des dépôts privés utilisés comme sources pour lancer des mineurs de crypto-monnaie.
Les acteurs de la menace ont été observés en train d'effectuer du cryptojacking dans les instances AWS Fargate et SageMaker, ce qui entraîne des coûts de calcul importants pour les victimes.
Sysdig estime que les pertes quotidiennes potentielles dépassent les 10 000 dollars si AMBERSQUID cible toutes les régions AWS.
Les attaquants ont engrangé plus de 18 300 dollars de revenus grâce à cette opération.
Bien que ce ne soit pas la première fois que des acteurs indonésiens sont liés à des campagnes de cryptojacking, il semble que cette attaque soit différente des précédentes.
Michael Clark, directeur de la recherche sur les menaces chez Sysdig, note que bien qu'il existe une communauté florissante d'attaquants de cryptojacking en Indonésie, les tactiques, techniques et procédures (TTP) d'AMBERSQUID ne se recoupent pas de manière significative avec les attaques précédentes menées par des acteurs indonésiens de la menace. Cela suggère que des groupes différents sont probablement responsables de ces campagnes.
L'opération AMBERSQUID souligne l'importance de prendre en compte la sécurité des services AWS moins courants, car ils peuvent fournir un accès indirect aux ressources informatiques et peuvent être négligés du point de vue de la sécurité en raison de leur moindre visibilité par rapport aux services informatiques traditionnels tels que EC2.

Source : *https://bit.ly/46awPjP*

Bon à savoir

Ne jamais utiliser le mot de passe maître comme mot de passe pour d'autres comptes

Un récent sondage en ligne mené par Security.org auprès de 1 051 adultes américains révèle qu'un Américain sur trois utilise désormais des gestionnaires de mots de passe, ce qui représente une augmentation significative par rapport à 2022 (un Américain sur cinq). Les gestionnaires de mots de passe sont choisis pour diverses raisons, notamment la gestion de plusieurs comptes sur différents appareils, le renforcement de la sécurité et le confort de ne pas avoir à mémoriser des mots de passe complexes.

L'enquête indique que les logiciels de gestion de mots de passe sont principalement installés sur des smartphones, mais qu'il y a eu une augmentation d'année en année des installations sur des ordinateurs portables, des ordinateurs de bureau, des tablettes et d'autres appareils. En particulier, trois quarts des abonnés utilisent des gestionnaires de mots de passe sur des ordinateurs personnels, et 71 % les déploient sur plusieurs appareils.

L'adoption des gestionnaires de mots de passe dans le cadre professionnel est également en hausse, avec 58 % des adultes utilisant ces services pour les références professionnelles, contre 50 % l'année précédente.

Les gestionnaires de mots de passe les plus populaires sont Google Password Manager et iCloud Keychain d'Apple, principalement en raison de leur caractère intégré, pratique et gratuit. Toutefois, la popularité de LastPass a diminué en raison des violations de données survenues en 2022 et 2023.

Les utilisateurs attendent des gestionnaires de mots de passe qu'ils soient pratiques, sûrs (avec des fonctionnalités telles que la biométrie et la sauvegarde hors ligne) et gratuits ou d'un prix raisonnable. Ils ont également tendance à privilégier les marques qu'ils utilisent déjà et en lesquelles ils ont confiance, et sont influencés par les recommandations de leurs amis et de leur famille, ainsi que par les avis positifs en ligne.

Malgré l'adoption croissante des gestionnaires de mots de passe, l'enquête met en évidence une tendance préoccupante : 28 % des utilisateurs utilisent leur mot de passe principal comme mot de passe pour d'autres comptes. Cette pratique présente des risques importants pour la sécurité, car un pirate qui obtient un mot de passe réutilisé à la suite d'une violation par un tiers peut potentiellement ouvrir une brèche dans le compte du gestionnaire de mots de passe d'un utilisateur et accéder à tous ses identifiants de connexion.

Pour renforcer la sécurité, les mots de passe maîtres doivent être longs, mémorisables par l'utilisateur mais difficiles à deviner, et uniques. L'enquête révèle également que 10 % des personnes interrogées ont utilisé ou utilisent des clés de sécurité et des clés de passage pour sécuriser leurs comptes. Toutefois, une majorité d'Américains continuent de recourir à des méthodes peu sûres, telles que la mémorisation, les notes, les navigateurs et les fichiers non cryptés, pour gérer leurs informations d'identification.

Source : *https://bit.ly/3PXSK85*

Evènements

Evènement du mois

SECURA North Africa

19-21 Septembre 2023

Safex Alger, ALgérie

https://bit.ly/3LKumnP

Secura North Africa revient pour sa 5ème édition du salon international de la sûreté, de la sécurité, du feu, et de l'urgence. Le salon a été organisé en Algérie, l'objectif de cet événement été de rassembler au même endroit pendant 3 jours tous les acteurs et professionnels du secteur de la sécurité industrielle et commerciale, de la sécurité des travailleurs, de la lutte contre l'incendie et des urgences.

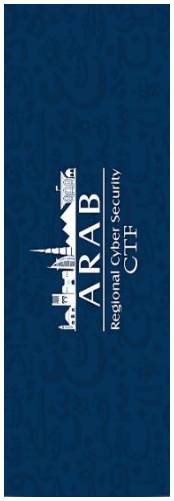
Evènement à venir

Arab Regional Cybersecurity CTF 2023

21 Octobre 2023

Online

https://bit.ly/48Can4M



En coopération avec Trend Micro en tant que partenaire stratégique, CyberTalents organise le CTF régional arabe de cybersécurité pour la 7ème année consécutive, rassemblant tous les talents arabes pour concourir dans un événement de grande envergure où plus de 22 pays arabes participeront, notamment les Émirats arabes unis, le Bahreïn, Djibouti, l'Algérie, l'Égypte, la Tunisie, le Yémen et bien d'autres encore.

Référence	ANPT-2023-BV-09
Titre	Bulletin de veille N°09
Date de version	30 Septembre 2023
Contact	ssi@anpt.dz