BULLETIN DE VEILLE N°05

ANPT-2023-BV-05

"To competently perform rectifying security service, two critical incident response elements are necessary: information and organization."
- Robert Davis-

Mai 2023

Alertes de sécurité

Cisco

Cisco déclare que des exploits PoC sont disponibles pour les vulnérabilités des commutateurs d'entreprise récemment corrigées

18 Mai 2023

Cisco a annoncé des correctifs pour des vulnérabilités de gravité critique dans plusieurs commutateurs pour petites entreprises et a averti qu'un code de preuve de concept (PoC) les ciblant existe publiquement.

Identifiées dans l'interface utilisateur web des commutateurs concernés, les failles peuvent être exploitées à distance, sans authentification, pour exécuter un code arbitraire avec les privilèges de l'utilisateur principal.

Répertoriées comme CVE-2023-20159, CVE-2023-20160, CVE-2023-20161 et CVE-2023-20189, ces vulnérabilités ont un score CVSS de 9,8.

Cisco a aussi publié des mises à jour logicielles pour cinq autres failles de haute gravité qui peuvent être exploitées via des requêtes élaborées. Quatre d'entre elles peuvent entraîner un déni de service, tandis que la cinquième permet aux attaquants de lire des informations non autorisées.

Les failles ont été corrigées avec la publication de la version 2.5.9.16 du micrologiciel pour les commutateurs intelligents de la série 250, les commutateurs gérés de la série 350 et les commutateurs gérés empilables des séries 350X et 550X, et avec la version 3.3.0.16 du micrologiciel pour les commutateurs intelligents de la série 250 et les commutateurs gérés de la série 350 pour les entreprises.

Les commutateurs intelligents de la série 200, les commutateurs gérés de la série 300 et les commutateurs gérés empilables de la série 500 pour les petites entreprises sont également concernés, mais Cisco ne prévoit pas de mettre à jour ces appareils, étant donné qu'ils sont entrés dans le processus de fin de vie (EoL).

Cisco a également annoncé des correctifs pour plusieurs bogues de gravité moyenne dans le logiciel IOS XE ROM Monitor (ROMMON), Smart Software Manager (SSM) On-Prem, Identity Services Engine (ISE), le logiciel DNA Center et les Business Wireless Access Points (APs).

Source : *https://bit.ly/43eKk0g*

Chrome 113

La mise à jour de sécurité Chrome 113 corrige une vulnérabilité critique

17 Mai 2023

Google a publié une mise à jour de sécurité de Chrome 113 qui résout un total de 12 vulnérabilités, dont une classée "critique". Six de ces failles ont été signalées par des chercheurs externes.
Identifiée sous le nom de CVE-2023-2721 et signalée par Guang Gong, chercheur à Qihoo 360, la faille est décrite comme une faille "use-after-free" dans Navigation.
Un attaquant peut créer une page HTML pour déclencher une corruption du tas lorsqu'un utilisateur accède à la page. L'attaquant devrait convaincre l'utilisateur de visiter la page.
Dans Chrome, les problèmes de type "use-after-free" peuvent être exploités pour échapper au Sandbox du navigateur, ce qui nécessite également pour l'attaquant de cibler une vulnérabilité dans le système sous-jacent ou dans le processus du navigateur de Chrome.
Trois autres failles de type "use-after-free" ont été corrigé, toutes classées comme étant d'une gravité "élevée". Ces vulnérabilités affectent les composants Autofill UI, DevTools et Guest View du navigateur.
La nouvelle version du navigateur résout également un bogue de confusion de type de gravité élevée dans le moteur JavaScript V8 et un problème d'implémentation inappropriée de gravité moyenne dans les WebApp Installs.
Google indique qu'il a versé 11 500 dollars de primes aux chercheurs qui l'ont informé de l'existence de ces bogues.
La dernière itération de Chrome est maintenant déployée en tant que version 113.0.5672.126 pour macOS et Linux, et en tant que versions 113.0.5672.126/.127 pour Windows.

Source : *https://bit.ly/3qdS9oj*

Apple

Apple corrige trois failles permettant de pirater des iPhones et des Macs

18 Mai 2023

Apple a corrigé trois nouvelles failles de type "zero-day" qui étaient utilisées pour s'introduire dans les systèmes iPhone, Mac et iPad.

Les trois failles de sécurité, qui ont toutes été découvertes dans le moteur de navigateur multiplateforme WebKit, sont répertoriées sous les noms CVE-2023-32409, CVE-2023-28204 et CVE-2023-32373.

La première faille permet à des attaquants distants de sortir des bacs à sable de contenu Web. Il s'agit d'une vulnérabilité d'évasion de Sandbox.

Les deux autres, qui peuvent être exploitées en incitant les cibles à charger des pages web malveillantes, sont une lecture hors limites qui peut permettre aux attaquants d'accéder à des données privées et une faille "use-after-free" qui permet l'exécution de code arbitraire sur les appareils infectés.

Des améliorations ont été apportées aux contrôles de limites, à la validation des entrées et à la gestion de la mémoire dans macOS Ventura 13.4, iOS et iPadOS 16.5, tvOS 16.5, watchOS 9.5 et Safari 16.5 afin de remédier aux trois failles "zero-day".

La faille affecte à la fois les anciens et les nouveaux modèles :

iPhone 6s (tous les modèles), iPhone 7, iPhone SE (1ère génération), iPad Air 2, iPad mini (4ème génération), iPod touch (7ème génération), et iPhone 8 et suivants iPad Pro (tous les modèles), iPad Air (3ème génération et suivants), iPad (5ème génération et suivants), et iPad mini (5ème génération et suivants), Macs fonctionnant sous macOS Big Sur, Monterey, et Ventura, Apple TV 4K (toutes les versions), Apple TV HD et Apple Watch Series 4.

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

WordPress

La faille du plugin WordPress Field Builder exploitée dans des attaques deux jours après l'application du correctif

15 Mai 2023

Des acteurs de la menace ont été vus en train d'adopter un code d'exploitation de preuve de concept (PoC) public ciblant une vulnérabilité XSS (cross-site scripting) dans le plugin WordPress Advanced Custom Fields, deux jours seulement après la publication d'un correctif, selon Akamai.

Répertoriée sous le nom de CVE-2023-30777, cette vulnérabilité de haute sévérité pourrait permettre aux attaquants d'injecter des scripts malveillants et d'autres charges utiles dans les sites web vulnérables. Le code serait exécuté lorsque les visiteurs se rendent sur le site web.

Le problème peut être déclenché sur les installations de plugins par défaut et ne nécessite pas d'authentification pour une exploitation réussie.

CVE-2023-30777 a été corrigé avec la publication de la version 6.1.6 d'Advanced Custom Fields le 4 mai. Le correctif était également inclus dans la version 5.12.6 du plugin.

L'aspect le plus intéressant des attaques observées est le fait qu'elles utilisent le même exploit PoC que la société de sécurité WordPress Patchstack, qui a déjà identifié la vulnérabilité.

Avec plus de deux millions de sites web WordPress utilisant des champs personnalisés avancés, l'exploitation de CVE-2023-30777 va probablement se poursuivre. Il est conseillé aux utilisateurs de mettre à jour leurs installations dès que possible.

Source : *https://bit.ly/42d4mXB*

Adobe

Adobe corrige 14 vulnérabilités dans Substance 3D Painter

09 Mai 2023

Adobe a annoncé des mises à jour de sécurité pour son produit Substance 3D Painter afin de corriger plus d'une douzaine de vulnérabilités. Il s'agit du seul produit pour lequel le géant du logiciel a publié des mises à jour dans le cadre du Patch Tuesday.

Selon Adobe, le logiciel de peinture 3D, plus précisément la version 8.3.0 et les versions antérieures, est affecté par 14 vulnérabilités.

La grande majorité d'entre elles sont des vulnérabilités de haute gravité ("critiques" selon les classifications de sévérité d'Adobe) liées à la mémoire qui peuvent être exploitées pour exécuter un code arbitraire dans le contexte de l'utilisateur ciblé. Certains problèmes moins graves peuvent entraîner des fuites de mémoire.

Rien n'indique que ces failles aient été exploitées dans la nature. Le niveau de priorité attribué par l'entreprise suggère également qu'il est peu probable qu'elles soient un jour exploitées à des fins malveillantes.

Toutes ces vulnérabilités ont été signalées à Adobe par le chercheur Mat Powell dans le cadre de l'initiative "Zero Day" (ZDI) de Trend Micro.

M. Powell a récemment découvert des vulnérabilités similaires dans Substance 3D Designer et Substance 3D Stager d'Adobe. Ces vulnérabilités ont été corrigées par l'éditeur en avril et en mars, et la ZDI a déjà publié des avis pour chaque bogue de sécurité.

Les avis de ZDI indiquent que les failles peuvent être exploitées par un attaquant en incitant l'utilisateur ciblé à ouvrir un fichier spécialement conçu. Le même vecteur d'attaque s'applique probablement aux vulnérabilités de Substance 3D Painter.

Adobe gère sur HackerOne un programme privé de recherche de bogues sur invitation uniquement, mais les chercheurs qui souhaitent aider l'entreprise à trouver des failles dans ses produits peuvent contacter l'équipe de sécurité d'Adobe et fournir leur identifiant HackerOne.

Source : *https://bit.ly/3C2vAWm*

Actualité

Accès malveillant aux VMs grâce à la Serial Console d'Azure

La société Mandiant (une filiale de Google spécialisé en cybersécurité) a identifié un cybergang à motivation financière connu sous le nom de " UNC3944 " qui utilise des tactiques d'hameçonnage et d'échange de cartes SIM pour compromettre les comptes administrateurs Microsoft Azure et obtenir un accès non autorisé à des machines virtuelles. L'objectif du groupe est de voler des données aux organisations qui utilisent le service Microsoft Cloud.

UNC3944, précédemment associé à la création d'outils de résiliation de logiciels de sécurité, est actif depuis au moins mai 2022. Les attaquants s'appuient sur des informations d'identification volées lors d'attaques de phishing par SMS pour obtenir un accès initial aux comptes d'administration Azure. Ils se font ensuite passer pour des administrateurs et manipulent les agents du service d'assistance pour qu'ils fournissent des codes de réinitialisation multi-facteurs par SMS. En procédant à un échange de cartes SIM, les attaquants interceptent ces codes, ayant déjà porté le numéro de téléphone de l'administrateur sur leur propre appareil, sans que la victime ne se rende compte de la violation.

Une fois dans l'environnement Azure, UNC3944 utilise ses privilèges d'administrateur pour recueillir des informations, modifier les comptes Azure existants et en créer de nouveaux. Pour mener ses opérations en toute discrétion, le groupe emploie des tactiques de "survie", en particulier en utilisant les extensions Azure - des fonctions supplémentaires pour les machines virtuelles Azure qui étendent les capacités et automatisent les tâches. Les attaquants abusent des extensions de diagnostic Azure et tentent d'exploiter d'autres extensions à des fins de surveillance et de collecte de données, mêlant ainsi leurs activités aux opérations habituelles.

UNC3944 s'introduit ensuite dans les machines virtuelles par le biais de l'Azure Serial Console, obtenant ainsi un accès administratif complet et contournant les méthodes de détection traditionnelles au sein d'Azure. Les attaquants utilisent PowerShell pour améliorer la persistance des machines virtuelles et déploient des outils d'administration à distance disponibles dans le commerce, des applications signées qui fournissent un accès à distance sans déclencher d'alertes. Ils établissent un tunnel SSH inverse pour maintenir un accès furtif et persistant via un canal sécurisé, en configurant la redirection de port pour les connexions directes aux machines virtuelles Azure compromises. Enfin, les attaquants se connectent à l'aide d'identifiants de compte utilisateur compromis via le shell inversé, étendant ainsi leur contrôle dans l'environnement et exfiltrant des données.

Le rapport de Mandiant souligne la connaissance approfondie de l'environnement Azure par UNC3944 et sa capacité à exploiter les outils intégrés pour échapper à la détection. Ces éléments, combinés à leurs compétences en ingénierie sociale pour l'échange de cartes SIM, représentent un risque important. Les organisations qui ne comprennent pas suffisamment les technologies en nuage et qui mettent en œuvre des mesures de sécurité inadéquates, telles que l'authentification multifactorielle par SMS, offrent des opportunités à ces acteurs sophistiqués de la menace.

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

Des pirates chinois exploitent les routeurs TP-Link pour mener des attaques persistantes

Selon des chercheurs de Check Point, un acteur chinois appelé Mustang Panda mène des attaques ciblées contre des entités des affaires étrangères européennes depuis janvier 2023. L'analyse de ces intrusions a permis de découvrir un implant de micrologiciel spécialement conçu pour les routeurs TP-Link.

Cet implant se compose de plusieurs éléments malveillants, dont une porte dérobée personnalisée appelée "Horse Shell". Cette porte dérobée permet aux attaquants de conserver un accès permanent, d'établir une infrastructure anonyme et de se déplacer latéralement au sein des réseaux compromis. L'implant est agnostique au niveau du firmware, ce qui signifie que ses composants peuvent être intégrés dans diverses versions de firmware provenant de différents fournisseurs.

Check Point a suivi ce groupe de menace sous le nom de "Camaro Dragon", qui est également connu sous d'autres pseudonymes tels que BASIN, Bronze President, Earth Preta, HoneyMyte, RedDelta et Red Lich.

La méthode exacte utilisée pour déployer les images de microprogrammes altérés sur les routeurs compromis est actuellement inconnue. On soupçonne que l'accès initial a pu être obtenu en exploitant des failles de sécurité connues ou en utilisant des mots de passe par défaut ou facilement devinables.

L'implant Horse Shell, écrit en C++, permet aux attaquants d'exécuter des commandes shell arbitraires, de télécharger des fichiers et de relayer la communication entre différents clients. Le micrologiciel modifié dissimule également la capacité du routeur à flasher une autre image par l'intermédiaire de l'interface web, cachant ainsi toute indication d'altération.

Il est intéressant de noter que la porte dérobée du routeur semble cibler divers appareils sur des réseaux résidentiels et domestiques, ce qui laisse penser que les routeurs compromis sont utilisés pour créer un réseau maillé. Ce réseau vise à établir une "chaîne de nœuds" entre les infections principales et les serveurs de commande et de contrôle. En relayant les communications par un tunnel SOCKS, les attaquants introduisent une couche supplémentaire d'anonymat, ce qui rend plus difficile la détection et l'interruption de l'attaque.

Même si l'un des nœuds de la chaîne est compromis ou mis hors service, l'attaquant peut maintenir la communication avec le serveur de commande et de contrôle en acheminant le trafic via un autre nœud de la chaîne.

Cette technique consistant à utiliser des routeurs compromis pour atteindre des objectifs stratégiques n'est pas nouvelle pour les acteurs de la menace affiliés à la Chine. En 2021, l'Agence nationale de cybersécurité française (ANSSI) a révélé un ensemble d'intrusions orchestrées par APT31 (également connu sous le nom de Judgement Panda ou Violet Typhoon) qui utilisait des logiciels malveillants avancés appelés Pakdoor ou SoWat pour permettre la communication entre les routeurs infectés.
Ces récentes découvertes mettent en évidence la tendance actuelle des acteurs chinois à exploiter les dispositifs de réseau orientés vers l'internet et à modifier leur logiciel ou leur micrologiciel à des fins malveillantes.

Source : *https://bit.ly/3OMEX42*

Le malware CLR SqlShell cible les serveurs MS SQL

Une nouvelle campagne ciblant les serveurs Microsoft SQL (MS SQL) mal gérés est apparue, visant à propager le logiciel malveillant CLR SqlShell. Ce logiciel malveillant permet de déployer des mineurs de crypto-monnaie et des ransomwares. CLR SqlShell est similaire à un shell web et permet aux acteurs de la menace d'exécuter des commandes et de se livrer à des activités malveillantes sur un serveur MS SQL.
La méthode d'attaque découverte par l'AhnLab Security Emergency response Center (ASEC) consiste à utiliser des procédures stockées CLR pour installer des logiciels malveillants sur des serveurs MS SQL. Cette méthode rejoint d'autres techniques telles que la commande xp_cmdshell, qui génère un shell de commande Windows et exécute des instructions d'entrée. Les acteurs de la menace associés à LemonDuck, MyKings (également connu sous le nom de DarkCloud ou Smominru) et Vollgar ont déjà exploité des serveurs MS SQL exposés à Internet en utilisant des attaques par force brute et par dictionnaire pour exécuter des commandes xp_cmdshell, des procédures stockées OLE et des logiciels malveillants.
L'utilisation de procédures stockées CLR est un ajout récent à la boîte à outils des attaquants. Ils exploitent les routines SqlShell pour télécharger des charges utiles de niveau suivant, notamment Metasploit et des mineurs de crypto-monnaie tels que MrbMiner, MyKings et LoveMiner.
Les attaquants ont utilisé diverses versions de SqlShell, telles que SqlHelper, CLRSQL et CLR_module, pour élever les privilèges sur les serveurs compromis, lancer des ransomwares, des proxywares et mener des opérations de reconnaissance dans les réseaux ciblés.

SqlShell a la capacité d'installer des logiciels malveillants supplémentaires tels que des portes dérobées, des mineurs de monnaie et des logiciels mandataires. Il peut également exécuter des commandes malveillantes reçues d'acteurs de la menace, à l'instar d'un shell web.
Il est conseillé aux organisations de sécuriser et de gérer correctement leurs serveurs MS SQL afin de prévenir ces attaques et d'atténuer le risque de déploiement de logiciels malveillants, d'accès non autorisé et de compromission des données.

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

Bon à savoir

Les attaques utilisent davantage de pièces jointes HTML malveillantes dans les courriels

Des chercheurs alertent sur la menace croissante que représentent les fichiers HTML malveillants utilisés dans les attaques par courrier électronique. Ces fichiers représentent désormais 50 % de toutes les pièces jointes HTML envoyées par courrier électronique, soit deux fois plus que l'année précédente. Contrairement aux campagnes d'attaques massives, cette augmentation n'est pas due à l'envoi de la même pièce jointe à un grand nombre de destinataires. Le langage HTML est privilégié par les attaquants en raison de sa polyvalence et de son utilisation répandue dans les communications électroniques légitimes. Par exemple, les pièces jointes HTML ressemblant à des rapports générés par diverses applications et outils peuvent sembler inoffensives et contourner les filtres de sécurité du courrier électronique.
Les attaquants exploitent la flexibilité du HTML pour mener différents types d'attaques. Une tactique courante est l'hameçonnage d'informations d'identification, où les pièces jointes HTML imitent les pages de connexion de services populaires. Ces pièces jointes peuvent également contenir du code JavaScript pour rediriger les utilisateurs vers des sites web de phishing. Une autre approche consiste à inciter les utilisateurs à télécharger des fichiers secondaires qui contiennent en réalité des charges utiles de logiciels malveillants. Cette méthode a un taux de réussite plus élevé que les autres types de fichiers pour ce qui est d'échapper aux passerelles de sécurité des courriels. En plaçant le leurre directement devant l'utilisateur, les attaquants contournent la première couche de défense, laissant aux solutions de protection des points finaux le soin de détecter le fichier téléchargé.
Les chercheurs ont observé des cas où les fichiers HTML contiennent eux-mêmes des logiciels malveillants sophistiqués, notamment des scripts et des exécutables puissants. Cette approche autonome est de plus en plus répandue par rapport aux attaques reposant sur des fichiers JavaScript hébergés à l'extérieur.
L'analyse de Barracuda en mai 2022 a révélé que 21 % des pièces jointes HTML analysées étaient malveillantes, ce qui représente le taux le plus élevé parmi tous les types de fichiers. En mars de l'année suivante, ce chiffre était passé à 45,7 %.
Pour évaluer les données avec précision et éviter que les résultats ne soient faussés par des attaques à grande échelle, les chercheurs ont examiné le caractère unique des fichiers. Au cours de deux périodes spécifiques, des pics de fichiers HTML malveillants ont été détectés. Il s'est avéré qu'un quart et 85 % des pièces jointes pendant ces périodes, respectivement, étaient le résultat d'attaques uniques.

Pour atténuer les risques associés aux pièces jointes HTML malveillantes, Barracuda recommande d'utiliser des solutions de sécurité du courrier électronique qui évaluent l'ensemble du contexte du courrier électronique, et pas seulement la pièce jointe elle-même. Il est essentiel de former les employés à l'identification et au signalement des pièces jointes HTML suspectes, en particulier celles provenant de sources inconnues. Des outils et des processus de réponse aux incidents doivent être mis en place pour supprimer rapidement les pièces jointes malveillantes signalées dans toutes les boîtes aux lettres concernées.
Parmi les autres mesures visant à réduire les risques, citons la mise en œuvre de solutions d'authentification à deux facteurs et d'accès à confiance zéro. Ces solutions évaluent divers facteurs tels que les informations d'identification, les informations sur l'appareil, la localisation, le fuseau horaire et l'historique de l'utilisateur afin de limiter les brèches même si les utilisateurs sont victimes de phishing et de vol d'informations d'identification. La surveillance des comptes d'utilisateurs après l'ouverture de session permet de détecter toute activité suspecte et d'alerter l'équipe de sécurité.

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

Evènements

Evènement du mois

Guerre et identité numérique - L'impact sur l'économie numérique

30 Mai 2023

Online

https://bit.ly/45AbOb2

La cyberguerre est une guerre silencieuse qui se déroule à l'insu du public. La cyberguerre a le potentiel de faire des ravages sur les comptes, les infrastructures et les systèmes critiques des personnes. Face à l'évolution du paysage des cyberattaques, il est essentiel que les organisations abordent les cyberrisques de manière méthodique et investissent dans des contrôles qui protègent leur personnel et leurs actifs essentiels.

Ce webbinaire a le but d'établir une véritable confiance numérique avec les clients numériques, fournir une sécurité sans friction et améliorer la fidélité des clients et augmentez la croissance numérique.

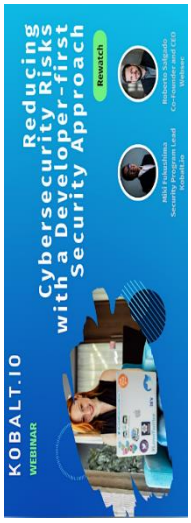
Evènement à venir

Réduire les risques de cybersécurité grâce à une approche de sécurité privilégiant les développeurs

01 Juin 2023

Online

https://bit.ly/3WUX0Y1



Les solutions basées sur le cloud permettent de réaliser des économies et des gains d'efficacité, mais elles peuvent également constituer une cible attrayante pour les acteurs de la menace. Les développeurs doivent fermer ces portes et les sécuriser à l'aide d'une approche de la sécurité axée sur le développeur. Les tests de sécurité ne peuvent plus être effectués après la production du code. La sécurité doit être intégrée dans tous les aspects d'une approche DevSecOps pour sécuriser le développement d'applications.

Dans ce webinaire, Roberto Salgado, cofondateur de Websec et Miki Fukushima, responsable du programme de sécurité de Kobalt.io discuteront la route vers DevSecOps.

Référence	ANPT-2023-BV-05
Titre	Bulletin de veille N°05
Date de version	31 Mai 2023
Contact	ssi@anpt.dz