BULLETIN DE VEILLE N°11

ANPT-2023-BV-11

« Technology trust is a good thing, but control is a better one »
- Stephane Nappo -

Novembre 2023

Alertes de sécurité

Chrome

Chrome : une faille de type 'zero-day' activement exploitée

29 Novembre 2023

Google a publié des mises à jour de sécurité pour résoudre sept problèmes dans son navigateur Chrome, dont une vulnérabilité de type "zero-day" (CVE-2023-6345) qui a été activement exploitée. Cette faille de haute gravité, identifiée comme un débordement d'entier dans la bibliothèque graphique Skia 2D, a été découverte et signalée par Benoît Sevens et Clément Lecigne du groupe d'analyse des menaces de Google le 24 novembre 2023.

Reconnaissant l'existence d'un exploit dans la nature pour CVE-2023-6345, Google s'est abstenu de divulguer des informations détaillées sur les attaques ou les acteurs de la menace impliqués. Notamment, une faille similaire de débordement d'entier dans le composant Skia (CVE-2023-2136) a été corrigée en avril 2023 après avoir été exploitée en tant que zero-day. Cela soulève la possibilité que CVE-2023-6345 puisse servir à contourner le correctif pour la vulnérabilité précédente.

La CVE-2023-2136 permettait à un attaquant distant qui compromettait le processus de rendu d'effectuer potentiellement une évasion du bac à sable via une page HTML conçue. La récente mise à jour corrige un total de six vulnérabilités zero-day dans Chrome depuis le début de l'année, chacune identifiée par un score CVSS (Common Vulnerability Scoring System) spécifique.

Il est vivement conseillé aux utilisateurs de mettre à jour leur navigateur Chrome vers la version 119.0.6045.199/.200 pour Windows et 119.0.6045.199 pour macOS et Linux afin d'atténuer les menaces potentielles. En outre, les utilisateurs de navigateurs basés sur Chromium, y compris Microsoft Edge, Brave, Opera et Vivaldi, devraient appliquer rapidement les correctifs disponibles pour renforcer la sécurité de leur navigateur. Des mises à jour régulières sont essentielles pour maintenir un environnement informatique sécurisé.

Source : *https://bit.ly/47wtpsd*

Zimbra

Une faille zero-day dans le logiciel de messagerie Zimbra exploitée par quatre groupes de hackers

16 Novembre 2023

Une vulnérabilité précédemment inconnue dans le logiciel de messagerie Zimbra Collaboration a été utilisée par quatre groupes distincts dans des attaques réelles pour voler des données de messagerie, des identifiants d'utilisateur et des jetons d'authentification. La faille, identifiée comme CVE-2023-37580, est une vulnérabilité XSS (cross-site scripting) réfléchie qui affecte les versions antérieures à 8.8.15 Patch 41. Bien que Zimbra ait publié des correctifs le 25 juillet 2023, le groupe d'analyse des menaces de Google (TAG) a observé de multiples campagnes d'exploitation de la vulnérabilité à partir du 29 juin 2023. L'exploit consiste à inciter les utilisateurs à cliquer sur une URL spécialement conçue, ce qui déclenche l'exécution d'un script malveillant dans le navigateur web de la victime. Les campagnes ont ciblé des organisations gouvernementales en Grèce, en Moldavie, en Tunisie et au Vietnam, l'une d'entre elles exploitant la faille pour obtenir des informations d'identification par hameçonnage. On a constaté que les acteurs de la menace exploitaient régulièrement les vulnérabilités XSS dans les serveurs de messagerie, ce qui souligne la nécessité de procéder à des audits approfondis et d'appliquer rapidement les correctifs. En outre, les campagnes ont mis en évidence la surveillance par les attaquants des dépôts de logiciels libres pour une exploitation opportuniste avant que les correctifs ne parviennent aux utilisateurs.

Source : *https://bit.ly/3R52hti*

Actualité

Contournement de l'authentification par empreinte digitale de Windows Hello

Des chercheurs en sécurité ont testé les capteurs d'empreintes digitales utilisés pour Windows Hello sur trois ordinateurs portables courants et ont réussi à trouver un moyen de contourner l'authentification sur chaque appareil.

Les cibles étaient un Dell Inspiron 15 équipé d'un capteur d'empreintes digitales Goodix, un Lenovo ThinkPad T14s équipé d'un capteur Synaptics et un Microsoft Surface Pro X équipé d'un capteur ELAN.

Les capteurs d'empreintes digitales intégrés et l'hôte ont été ciblés par des attaques logicielles et matérielles.

Tous les capteurs testés sont de type "Match-on-Chip", ce qui signifie que la puce est dotée d'un microprocesseur et d'une mémoire, et que les données d'empreintes digitales ne quittent jamais le capteur. La puce elle-même doit être attaquée afin de contourner l'authentification.

L'attaque nécessite un accès physique à l'appareil ciblé - l'attaquant doit voler l'appareil ou utiliser la méthode de la servante diabolique.

Les attaques démontrées par les chercheurs ont été menées en connectant un dispositif de piratage à chaque ordinateur portable, via USB, ou en connectant le capteur d'empreintes digitales à une plate-forme spécialement conçue à cet effet.

Pour les ordinateurs portables Dell et Lenovo, les chercheurs ont contourné l'authentification par empreinte digitale Windows Hello en identifiant les identifiants valides liés aux empreintes digitales de l'utilisateur et en enregistrant l'empreinte digitale de l'attaquant en imitant l'identifiant d'un utilisateur légitime.

Dans le cas de l'appareil Surface, l'attaquant doit débrancher le Type Cover, qui est essentiellement le clavier et comprend également le capteur d'empreintes digitales, et connecter un périphérique USB qui usurpe le capteur d'empreintes digitales et indique au système qu'un utilisateur autorisé est en train de se connecter.

Microsoft a partagé une présentation vidéo de la recherche lors de sa conférence BlueHat en octobre.

Source : *https://bit.ly/3Gpdj84*

L'index des paquets Python fait face à une crise de sécurité avec des fuites validées

Des chercheurs en sécurité ont découvert 3938 secrets uniques sur PyPI, le système officiel de gestion des paquets de la communauté Python, et en ont validé 768 comme étant authentiques. En particulier, 2922 projets ont hébergé au moins un secret unique, comprenant des informations d'identification telles que des clés AWS, des accès Redis, des clés d'API Google et diverses informations d'identification de bases de données. L'étude, dirigée par le développeur Python Tom Forbes et publiée sur GitGuardian, met en évidence les graves conséquences de ces fuites, en soulignant le rôle essentiel que jouent les informations d'identification valides dans les cyberattaques.

PyPI, qui héberge plus de 450 000 projets et constitue environ 90 % du code de production, fait partie intégrante de la chaîne d'approvisionnement en logiciels. Forbes souligne la nécessité de renforcer les mesures de sécurité en raison de l'inclusion croissante, par inadvertance, de secrets dans les logiciels libres.

L'étude révèle les tendances en matière de fuites de secrets, notant une augmentation des jetons de bot Telegram valides, des fuites de clés d'API Google et une augmentation des fuites d'identifiants de bases de données en 2022, suggérant que les fuites d'identifiants sont une cause majeure de brèches en 2023.

En outre, l'étude révèle que la plupart des secrets sont divulgués accidentellement. Forbes souligne la facilité avec laquelle un paquet destiné à un usage interne peut être mis par erreur à la disposition du public, ce qui revient à rendre public un repo privé. Le travail de sensibilisation réalisé dans le cadre du projet a permis de découvrir 15 incidents dans lesquels les éditeurs n'étaient pas conscients de la nécessité de rendre leurs projets publics, y compris des cas impliquant de grandes entreprises, ce qui souligne la nécessité d'une prise de conscience accrue et de mesures préventives.

L'exposition de secrets dans des paquets open-source présente des risques importants pour les développeurs et les utilisateurs, permettant aux attaquants d'obtenir un accès non autorisé, d'usurper l'identité des responsables ou de manipuler les utilisateurs par le biais de tactiques d'ingénierie sociale, comme indiqué dans le billet de blog.

.

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

Bon à savoir

Nouvelle technique de phishing

Les attaques de phishing évoluent, les cybercriminels adoptant des techniques avancées pour tromper les victimes et compromettre les informations sensibles. En 2023, une tendance notable est l'utilisation de codes QR, de CAPTCHA et de stéganographie, ce qui pose de nouveaux défis en matière de détection et de prévention.

Le "Quishing", une technique combinant les codes QR et le phishing, a gagné en popularité parmi les cybercriminels en 2023. En dissimulant des liens malveillants dans les codes QR, les attaquants peuvent contourner les filtres anti-spam traditionnels conçus pour les tentatives d'hameçonnage basées sur le texte. La complexité des codes QR constitue un défi pour les outils de sécurité, ce qui fait de cette méthode un choix privilégié pour les cybercriminels. Il existe plusieurs solutions qui permet aux utilisateurs d'analyser les codes QR dans un environnement sécurisé, dévoilant ainsi les URL cachées.

Les attaques basées sur les CAPTCHA exploitent les CAPTCHA, une mesure de sécurité sur les sites web, pour masquer les formulaires de collecte d'informations d'identification sur de faux sites web. Les attaquants exploitent les algorithmes générés par domaine aléatoire (RDGA) et les CAPTCHA de CloudFlare pour dissimuler ces formulaires aux systèmes de sécurité automatisés. Un exemple cible les employés de Halliburton Corporation, impliquant une vérification CAPTCHA et une page de connexion Office 365 réaliste. Une fois que les victimes ont saisi leurs informations d'identification, elles sont redirigées vers un site légitime, tandis que les attaquants exfiltrent les informations.

La stéganographie, qui consiste à dissimuler des données dans divers supports, est utilisée dans les attaques de phishing, en commençant par un courriel convaincant. Celui-ci contient une pièce jointe, souvent un document Word, et un lien vers une plateforme de partage de fichiers. En cliquant sur le lien, on télécharge une archive contenant un fichier script VBS. Une fois exécuté, le script récupère un fichier image d'apparence inoffensive contenant un code malveillant caché, qui infecte le système de la victime.

Source : *https://bit.ly/3uRg3rS*

Evènements

Evènement à venir

Cybersécurité : outils et solutions pratiques pour les PME

13 Décembre 2023

Online

https://bit.ly/47LJ0V6

L'**Agence du Numérique**, l'**Infopole**, l'**Union Wallonne des entreprises** et **Wallonie Entreprendre** organisent, dans le cadre du programme **Cyberwal by Digital Wallonia**, un webinaire sur le thème de la cybersécurité à destination des PME. Ce webinaire s'inscrit dans la continuité de l'événement de sensibilisation organisé pendant la Cyberweek 2023.

Ce webinaire a pour objectif de proposer des solutions concrètes aux entreprises qui souhaitent se cybersécuriser. Cette session en ligne vous permettra d'acquérir des connaissances sur les aides et des financements disponibles, de recevoir des conseils pratiques, d'assister à une démonstration d'une PME fictive qui se cybersécurise et surtout, de protéger votre entreprise des cyberattaques.

Référence	ANPT-2023-BV-11
Titre	Bulletin de veille N°11
Date de version	30 Novembre 2023
Contact	ssi@anpt.dz