BULLETIN DE VEILLE N°12

ANPT-2023-BV-12

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

Décembre 2023

Alertes de sécurité

Mozilla

Mozilla corrige plusieurs failles dans ses produits

20 Décembre 2023

Mozilla a publié des mises à jour de sécurité pour Firefox et Thunderbird afin de corriger un total de 20 vulnérabilités. Firefox 121 comprend des correctifs pour 18 failles, dont cinq ont un niveau de gravité élevé. L'une d'entre elles est la CVE-2023-6856, un débordement de mémoire tampon dans WebGL, l'API JavaScript pour le rendu des graphiques interactifs, qui pourrait conduire à l'exécution de code à distance et à l'évasion du bac à sable.

Une autre faille importante est la CVE-2023-6135, qui affecte les courbes NIST des services de sécurité du réseau (NSS) et les rend sensibles à l'attaque par canal latéral Minerva, permettant potentiellement aux attaquants de récupérer des clés privées à long terme. Mozilla a également corrigé la CVE-2023-6865, un bogue dans EncryptingOutputStream qui pourrait exposer des données non initialisées, ce qui pourrait avoir un impact sur le mode de navigation privée.

Firefox 121 corrige également les problèmes de sécurité de la mémoire identifiés comme CVE-2023-6873 et CVE-2023-6864, ce dernier affectant également Firefox ESR et Thunderbird. Huit failles de gravité moyenne, dont des problèmes de débordement de mémoire tampon du tas, d'utilisation après libération et d'évasion du bac à sable, ont également été résolues, ainsi que cinq faibles bogues.

Parallèlement, Thunderbird 115.6 a été publié avec des correctifs pour 11 vulnérabilités, dont neuf ont également été corrigées dans Firefox. Les deux autres failles de Thunderbird, d'une grande gravité, pourraient permettre à des attaquants d'usurper des messages électroniques (CVE-2023-50762) ou de manipuler l'heure à laquelle un message a été envoyé (CVE-2023-50761).

Il est conseillé aux utilisateurs de mettre à jour leurs installations Firefox et Thunderbird avec les versions les plus récentes pour garantir la sécurité.

Source : https://bit.ly/3TH2jdI

Google

Google a signalé un nouveau bogue 'zero-day' activement exploité dans Chrome

20 Décembre 2023

Google a publié des mises à jour d'urgence pour son navigateur web Chrome afin de corriger une vulnérabilité zero-day récemment découverte, identifiée comme CVE-2023-7024. Cette faille, un problème de débordement de la mémoire tampon du tas dans WebRTC, a été rapidement corrigée dans la version 120.0.6099.129 pour Mac et Linux, ainsi que dans les versions 120.0.6099.129 et 130 pour Windows.

Google a réussi à corriger le problème suivi sous le nom de CVE-2023-7024 (un débordement de mémoire tampon dans WebRTC) et note qu'un exploit existe déjà dans la nature, ce qui indique que la vulnérabilité a été activement ciblée. Toutefois, Google n'a pas fourni de détails spécifiques sur les attaques exploitant la faille.

La découverte de la vulnérabilité par le groupe d'analyse des menaces de Google suggère l'implication potentielle d'un acteur national ou d'une société de surveillance. Google limite généralement l'accès aux détails des bogues et aux liens jusqu'à ce qu'une majorité d'utilisateurs aient mis à jour leurs systèmes avec le correctif. Cette pratique permet d'atténuer le risque d'une exploitation généralisée pendant que les utilisateurs mettent à jour leur logiciel.

Cette vulnérabilité est le huitième problème corrigé par Google dans Chrome depuis le début de l'année. Les autres vulnérabilités zero-day activement exploitées dans Chrome et corrigées par Google au cours de la même période sont les suivantes : CVE-2023-2033, CVE-2023-2136, CVE-2023-3079, CVE-2023-4863, CVE-2023-5217, CVE-2023-6345 et CVE-2023-4762, couvrant divers types de problèmes de sécurité tels que la confusion de type, le débordement d'un entier et le débordement de la mémoire tampon d'un tas.

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

Actualité

Nouvelle attaque de phishing qui vole les codes de sauvegarde d'Instagram

Une nouvelle campagne de phishing est apparue, se faisant passer pour un e-mail de "violation de droits d'auteur" afin d'inciter les utilisateurs d'Instagram à révéler leurs codes de sauvegarde pour l'authentification à deux facteurs (2FA). La campagne de phishing vise à contourner la protection 2FA configurée sur les comptes Instagram.

L'authentification à deux facteurs est une fonction de sécurité qui ajoute une couche supplémentaire de vérification lors de la connexion à un compte.

Cependant, si des acteurs de la menace volent ces codes de sauvegarde, ils peuvent potentiellement détourner des comptes Instagram en utilisant des appareils inconnus, même s'ils n'ont que les informations d'identification du compte. La nouvelle campagne de phishing tire parti de la violation des droits d'auteur en informant les destinataires que leur compte a été restreint en raison d'une violation des lois sur la propriété intellectuelle. L'e-mail de phishing invite les utilisateurs à cliquer sur un bouton pour faire appel de la décision, ce qui les conduit à des pages de phishing où ils saisissent les informations d'identification de leur compte et d'autres détails.

La dernière variante de cette attaque se fait passer pour Meta, la société mère d'Instagram, et avertit les utilisateurs de plaintes pour violation du droit d'auteur. Le site de phishing, déguisé en portail de violations de Meta, guide les victimes à travers un processus en plusieurs étapes, qui se termine par une demande de nom d'utilisateur, de mot de passe et de code de sauvegarde à 8 chiffres.

Malgré plusieurs signes de fraude, tels que l'adresse de l'expéditeur, la page de redirection et les URL de la page de phishing, la campagne s'appuie sur une conception convaincante et un sentiment d'urgence qui pourrait tromper un grand nombre de cibles et les amener à divulguer leurs identifiants de compte et leurs codes de sauvegarde.

Il est rappelé aux utilisateurs de traiter les codes de sauvegarde avec le même niveau de confidentialité que les mots de passe et de ne les saisir que sur le site ou l'application Instagram officielle. Il est essentiel de rester vigilant face aux tentatives d'hameçonnage et de ne pas partager d'informations sensibles par le biais de canaux inconnus ou suspects.

Source : *https://bit.ly/41E721Z*

Une application android expose les mots de passe des utilisateurs

L'application Android "Barcode to Sheet", qui a été téléchargée plus de 100 000 fois sur Google Play et a reçu une note de 4,5 étoiles, expose les données sensibles des utilisateurs et des entreprises en raison d'une instance ouverte non vérifiée. Découverte par l'équipe de Cybernews, l'application sert de scanner de codes-barres, permettant aux utilisateurs de transférer des données à partir de codes-barres vers des formats compatibles avec les tableurs.

Les développeurs de l'application ont négligé de sécuriser leur base de données Firebase, laissant plus de 368 Mo de données accessibles à tous. Firebase est un service de stockage de données en temps réel couramment utilisé pour stocker les données collectées par les applications. Les données exposées comprenaient des informations d'entreprise sensibles stockées en clair, comprenant des détails sur les produits, les rapports, les courriels et les identifiants des utilisateurs. Les mots de passe des utilisateurs étaient stockés dans le format de hachage MD5, qui, malgré la sécurité qu'il est censé offrir, présente des vulnérabilités connues et est relativement facile à pirater.

Le serveur ouvert a également stocké des informations potentiellement sensibles du côté client de l'application, notamment des clés d'accès et des identifiants tels que l'identifiant du client web, la clé API de Google, l'identifiant de l'application Google, la clé de signalement des pannes et d'autres données destinées uniquement aux développeurs de l'application. L'accès non autorisé à ces informations peut conduire à des attaques par hameçonnage, à un accès non autorisé aux services et à des dommages potentiels pour les utilisateurs.

L'équipe de Cybernews a souligné la sensibilité des données divulguées, qui comprennent des secrets d'application, des informations d'entreprise et des données d'utilisateur, y compris des mots de passe. La quantité considérable de données exposées par une application comptant moins d'un demi-million d'utilisateurs soulève des inquiétudes quant à une éventuelle utilisation abusive par des acteurs menaçants. Les données volées se retrouvent souvent sur le dark web, où elles peuvent être exploitées à des fins financières, d'usurpation d'identité, de phishing et de credential stuffing. Les cybercriminels peuvent utiliser les informations d'identification personnelle divulguées à diverses fins malveillantes, ce qui représente un risque pour les personnes concernées.

Source : *https://bit.ly/41FoZgu*

Bon à savoir

Les vulnérabilités sont désormais le premier moyen d'accès aux ransomwares

Une analyse récente de Corvus Insurance (compagnie d'assurance cybernétique qui offre une couverture sur mesure, des devis basés sur des données et des conseillers en risques à la demande pour les cyber-risques complexes) révèle un changement de tactique chez les acteurs de la menace en ce qui concerne les attaques par ransomware. Les données indiquent une augmentation de l'exploitation

des vulnérabilités comme méthode d'accès initiale, s'éloignant de la dépendance traditionnelle aux courriels de phishing. Plus précisément, l'exploitation des vulnérabilités représentait près de 0 % des demandes d'indemnisation pour ransomware au second semestre 2022, puis près d'un tiers au premier semestre 2023. L'assureur a souligné que les grandes campagnes exploitant les vulnérabilités des logiciels de transfert de fichiers MOVEit et GoAnywhere ont contribué à cette évolution.

En outre, Corvus a souligné l'utilisation croissante de clés cryptographiques exposées comme une autre voie pour les acteurs de la menace de compromettre les organisations. L'analyse a révélé que 7 % des organisations étudiées avaient au moins un secret exposé, les clés API de Google, les jetons web JSON, les clés de domaine Shopify et les clés des buckets S3 d'AWS étant les plus courantes. Le rapport souligne que si toutes les expositions ne présentent pas un risque important, environ 1 % des organisations avaient des clés exposées jugées "critiques" par les experts en sécurité, nécessitant une attention immédiate. Ces expositions critiques comprenaient des clés d'API AWS, des clés de stockage en nuage et des clés d'API pour divers services de fournisseurs non en nuage tels que LinkedIn, Okta, Slack, MailChimp, Facebook, New Relic, Stripe et Sauce Labs.

Corvus a également noté que l'ingénierie sociale est devenue une cause importante de réclamations d'assurance, représentant près de la moitié de toutes les réclamations au troisième trimestre 2023, contre environ 35-38 % un an plus tôt. L'ingénierie sociale est ainsi responsable de près de trois fois plus de sinistres que la catégorie suivante, à savoir les atteintes à la sécurité des fournisseurs ou d'autres tiers. Il est intéressant de noter qu'aucun cas de violation liée à l'ingénierie sociale n'a été signalé parmi les assurés de Google Workspace, alors que Microsoft est à l'origine de la majorité de ces incidents.

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

Evènements

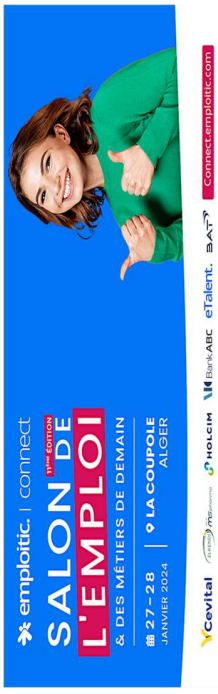
Evènement à venir

Cybersécurité : outils et solutions pratiques pour les PME

27-28 Janvier 2024

La Coupole d'Alger

https://bit.ly/3H3VZFC



La 11ème édition du salon Connect aura lieu à la Coupole d'Alger !

A la recherche d'un premier emploi ou ayant des aspirations professionnelles, le salon Emploitic Connect est un rendez-vous à ne pas manquer. Le Salon permet de rencontrer plus de 100 entreprises et d'explorer des milliers d'opportunités de carrière.

Pourquoi participer ?

- Accède à de nombreuses offres d'emploi dans divers secteurs et métiers.
- Rencontre des recruteurs, élargis ton réseau professionnel et saisis des opportunités.
- Participe à des ateliers et conférences pour bénéficier de conseils pour propulser ta carrière.

Référence	ANPT-2023-BV-12
Titre	Bulletin de veille N°12
Date de version	31 Décembre 2023
Contact	ssi@anpt.dz