BULLETIN DE VEILLE N°10

ANPT-2023-BV-10

«It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it. »
- Stephane Nappo -

Octobre 2023

Alertes de sécurité

Oracle

Oracle corrige 185 vulnérabilités avec l'unité centrale d'octobre 2023

18 Octobre 2023

Oracle a annoncé la publication de 387 nouveaux correctifs de sécurité dans le cadre de l'unité centrale de traitement d'octobre 2023, afin de résoudre les vulnérabilités affectant son propre code et des composants tiers.

Plus de 40 correctifs de sécurité concernent des failles de gravité critique et plus de 200 résolvent des bogues qui peuvent être exploités à distance sans authentification.

SecurityWeek a identifié 185 CVE uniques dans l'unité centrale d'Oracle d'octobre 2023.

Le produit Oracle ayant reçu le plus grand nombre de correctifs de sécurité est Financial Services Applications, avec 103 correctifs, dont 49 concernent des vulnérabilités exploitables à distance sans authentification.

Vient ensuite Oracle Communications, avec 91 correctifs de sécurité, dont 60 concernent des problèmes non authentifiés et exploitables à distance.

Oracle a également annoncé de nombreux correctifs pour Fusion Middleware (46 correctifs - 35 pour des vulnérabilités qui peuvent être exploitées par des attaquants non authentifiés à distance) et MySQL (37-9).

Des correctifs ont également été publiés pour Analytics (16-11), Retail Applications (15-9), Database Server (10-2), Communications Applications (9-4), Commerce (6-5), GoldenGate (6-3), Enterprise Manager (5-5), Java SE (5-5), PeopleSoft (5-3), E-Business Suite (4-3), Construction and Engineering (4-1), Systems (3-2), Utilities (3-2), Health Sciences Applications (2-2), Siebel CRM (2-2), Hyperion (2-1), Hospitality Applications (2-0), Essbase (1-1), REST Data Services (1-1), JD Edwards (1-1), Supply Chain (1-1), Secure Backup (1-0), TimesTen In-Memory Database (1-0), HealthCare Applications (1-0), et Insurance Applications (1-0).

Oracle encourage ses clients à appliquer ces correctifs de sécurité dès que possible. Pour les clients qui ont omis un ou plusieurs processeurs, Oracle recommande de consulter les mises à jour de sécurité publiées précédemment pour déterminer si leurs produits nécessitent un correctif.

Source : *https://bit.ly/3MgjY7D*

Chrome 118

Chrome 118 corrige 20 vulnérabilités

11 Octobre 2023

Google a annoncé la mise à disposition de Chrome 118 sur le canal stable, avec des correctifs pour 20 vulnérabilités, dont 14 signalées par des chercheurs externes.

La plus grave des failles signalées par des chercheurs externes est la CVE-2023-5218, un bogue critique décrit comme un problème d'utilisation après libération dans Site Isolation, le composant de Chrome chargé d'empêcher les sites de voler les données d'autres sites.

Mis en œuvre dans Chrome en tant que mesure de sécurité supplémentaire, Site Isolation regroupe les pages de différents domaines dans des processus différents qui s'exécutent dans leurs propres Sandboxes.

Chrome 118 résout également huit failles de gravité moyenne, dont six sont des problèmes d'implémentation inappropriés dans les API Fullscreen, Navigation, DevTools, Intents, Downloads et Extensions.

Une vulnérabilité de type "use-after-free" dans Blink History et un débordement de mémoire tampon dans PDF, tous deux de gravité moyenne, ont également été résolus.

Les cinq autres problèmes corrigés sont des vulnérabilités de faible gravité : quatre implémentations inappropriées et une utilisation après suppression.

Le géant de l'internet ne fait aucune mention de l'exploitation de ces vulnérabilités dans le cadre d'attaques malveillantes.

La dernière version de Chrome est maintenant disponible sous la forme de la version 118.0.5993.70 pour macOS et Linux, et sous la forme des versions 118.0.5993.70/.71

Source : *https://bit.ly/491m3hH*

Actualité

D-Link : Déclaration de violation de données qui a touché l'entreprise

D-Link, fabricant taïwanais d'équipements de réseau, a reconnu avoir été victime d'une violation de données qui a conduit à l'exposition de ce qu'il a déclaré être des "informations semi-publiques et peu sensibles".

Selon l'entreprise, les données ont été confirmées comme non provenant du Cloud, mais probablement d'un ancien système D-View 6, qui a atteint sa fin de vie dès 2015.

Les données ont été utilisées à des fins d'enregistrement à l'époque. Jusqu'à présent, rien n'indique que ces données obsolètes contenaient des identifiants d'utilisateurs ou des informations financières.

Ce développement intervient plus de deux semaines après qu'une partie non autorisée ait prétendument volé les données personnelles de nombreux fonctionnaires du gouvernement taïwanais ainsi que le code source du logiciel de gestion de réseau D-View de D-Link dans un message partagé sur BreachForums le 1er octobre 2023.

D-Link, qui a fait appel à la société de cybersécurité Trend Micro pour enquêter sur l'incident, a cité de nombreuses inexactitudes et exagérations, affirmant que la violation avait entraîné la compromission d'environ 700 enregistrements "obsolètes et fragmentés", contrairement aux affirmations selon lesquelles des millions de données d'utilisateurs avaient été détournées.

" Il y a des raisons de croire que les derniers horodatages de connexion ont été intentionnellement trafiqués pour que les données archaïques paraissent récentes ", a indiqué l'entreprise.

L'entreprise a également indiqué que la violation était due à un employé victime par inadvertance d'une attaque par hameçonnage et qu'elle prenait des mesures pour renforcer la sécurité de ses opérations. Les détails exacts de l'attaque n'ont pas été divulgués.

L'entreprise a également souligné que ses clients actifs actuels ne devraient pas être affectés par cet incident.

Source : https://bit.ly/3QGB403

Casio révèle une violation de données touchant des clients dans 149 pays

Casio, le fabricant japonais d'électronique, a signalé une violation de données touchant des clients de 149 pays. La faille a été détectée le 11 octobre lorsque la base de données de la plateforme éducative ClassPad a rencontré des problèmes dans l'environnement de développement de l'entreprise. Les preuves suggèrent que le pirate a eu accès aux informations des clients le 12 octobre. Les données compromises comprennent les noms des clients, leurs adresses électroniques, les pays de résidence, les détails d'utilisation des services, et les informations d'achat, à l'exception des informations de cartes de crédit.

Jusqu'au 18 octobre, les pirates ont accédé à 91 921 éléments appartenant à des clients japonais et à 35 049 enregistrements de clients dans 148 pays en dehors du Japon. Casio a expliqué que des erreurs opérationnelles et une gestion opérationnelle insuffisante ont désactivé certains paramètres de sécurité dans l'environnement de développement, permettant ainsi à des tiers non autorisés d'accéder aux données.

Malgré la compromission de la base de données, l'application ClassPad.net est toujours en ligne, et les systèmes au-delà de la base de données compromise dans l'environnement de développement sont restés intacts. Le 16 octobre, Casio a signalé l'incident aux autorités japonaises et collabore avec les forces de l'ordre pour enquêter sur la violation. De plus, Casio travaille avec des experts en cybersécurité pour comprendre les causes de l'incident et mettre en place des mesures de protection.

En août, un individu menaçant nommé "thrax" a affirmé avoir divulgué plus de 1,2 million d'enregistrements d'utilisateurs prétendument volés depuis un serveur Remote Desktop Services (RDS) contenant d'anciennes bases de données de casio.com. Ces données remontent jusqu'en juillet 2011 et contiennent des clés AWS et des identifiants de base de données. Les détails supplémentaires concernant l'incident d'octobre et les affirmations de Thrax n'ont pas été confirmés par un porte-parole de Casio.

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

Bon à savoir

Plus de 40 000 comptes du portail d'administration utilisent "admin" comme mot de passe

Des chercheurs en sécurité ont identifié une préoccupation majeure en découvrant que de nombreux administrateurs informatiques utilisent des mots de passe faibles, voire par défaut, pour protéger l'accès aux portails, exposant ainsi les réseaux d'entreprise à des cyberattaques. L'analyse de plus de 1,8 million d'informations d'identification d'administrateur a révélé que plus de 40 000 d'entre elles utilisaient simplement le mot de passe "admin", suggérant une utilisation répandue des mots de passe par défaut.

Les données d'authentification ont été collectées entre janvier et septembre grâce à Threat Compass, une solution de renseignement sur les menaces proposée par la société de cybersécurité Outpost24. Ces informations d'authentification sont généralement extraites

par des logiciels malveillants spécialisés dans le vol de données, avec un intérêt particulier pour les applications stockant des noms d'utilisateur et des mots de passe.

Les chercheurs ont noté que la plupart des mots de passe figurant dans leur liste auraient pu être facilement devinés lors d'une attaque de devinette de mot de passe peu sophistiquée. Outpost24 a identifié les mots de passe les plus faibles utilisés pour les portails d'administration, et le top 20 comprend des choix de mots de passe extrêmement prévisibles tels que "admin," "123456," "mot de passe," et d'autres.

Les chercheurs mettent en garde contre le fait que ces mots de passe faibles sont associés aux portails d'administration, qui sont souvent ciblés par les acteurs de la menace, car ils permettent d'accéder à des configurations sensibles, des comptes, et des paramètres de sécurité. Pour renforcer la sécurité des réseaux d'entreprise, il est essentiel d'appliquer des principes de sécurité fondamentaux, notamment l'utilisation de mots de passe longs, robustes et uniques pour chaque compte, en particulier pour les utilisateurs disposant d'un accès à des ressources sensibles.

Outpost24 recommande également de recourir à des solutions de réponse aux points de terminaison et de détection pour se protéger contre les logiciels malveillants qui volent des informations. D'autres mesures de sécurité incluent la désactivation des options d'enregistrement et de remplissage automatique des mots de passe dans les navigateurs Web, la vérification des domaines lors des redirections, et l'abandon de l'utilisation de logiciels piratés.

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

Evènements

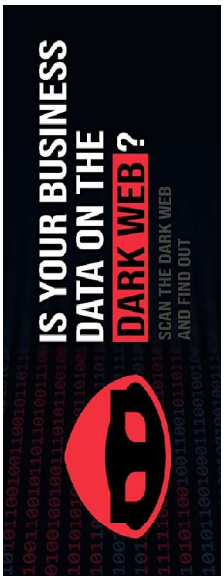
Evènement du mois

Développer son MSP grâce à la surveillance du Dark Web

31 Octobre 2023

Online

https://bit.ly/3SpvcKW



Selon les données de la National Cyber Security Alliance, près de la moitié (47 %) des petites et moyennes entreprises ont été touchées par des cyberattaques réussies, et parmi elles, 60 % ont été contraintes de suspendre leurs activités. Les intrusions informatiques, qui sont à l'origine de la plupart de ces attaques, reposent fréquemment sur l'utilisation de mots de passe volés ou faibles. Ces mots de passe sont souvent exposés sur le Dark Web et sont utilisés par les cybercriminels pour accéder aux comptes des employés au sein des applications internes de l'entreprise.

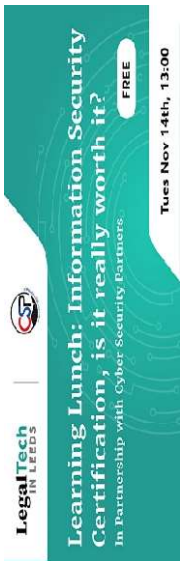
Evènement à venir

Information Security Certification - Is it Really worth it?

14 Novembre 2023

Online

https://bit.ly/3sjCxRK



Recevoir un badge est toujours gratifiant, car il symbolise une réussite et rassure vos clients sur vos compétences dans votre domaine.
Cependant, maintenir ces badges peut parfois s'avérer un défi, nécessitant une constante adaptation aux normes établies.
Que ce soit pour respecter les exigences de Cyber Essentials, se conformer aux normes internationales ou répondre aux normes spécifiques à un secteur, il est important de comprendre les retours sur investissement liés à la certification continue de l'organisation. Est-ce que les efforts en valent la peine, et quels avantages cela apporte-t-il, en dehors de la simple possession du badge ?
Kevin Else, Directeur de la Consultation chez Cyber Security Partners, explorera certains des coûts dissimulés et des avantages associés à l'acquisition et au maintien de certifications en matière de sécurité de l'information.

Référence	ANPT-2023-BV-10
Titre	Bulletin de veille N°10
Date de version	31 Octobre 2023
Contact	ssi@anpt.dz