BULLETIN DE VEILLE N°07

ANPT-2022-BV-07

"Technology trust is a good thing, but control is a better one."
— Stephane Nappo --

Juillet 2022

Alertes de sécurité

Cisco

Cisco corrige des failles de sécurité critiques affectant Nexus Dashboard

20 Juillet 2022

Cisco a publié des correctifs de sécurité pour 45 vulnérabilités affectant une variété de ses produits, dont une est classée comme étant critique et trois comme étant élevée.

Les problèmes les plus graves ont un impact sur Cisco Nexus Dashboard pour les centres de données et les infrastructures de réseau en cloud, et ils sont décrits comme suit :

- CVE-2022-20857 (score CVSS : 9.8) : Faille d'exécution de commandes arbitraires dans Cisco Nexus Dashboard ;
- CVE-2022-20858 (score CVSS : 8.2) : Faille de lecture et d'écriture d'image de conteneur de Cisco Nexus Dashboard ;
- CVE-2022-20861 (score CVSS : 8.8) : Faille CSRF (cross-site request forgery) de Cisco Nexus Dashboard.

Une autre faille de haute gravité concerne une vulnérabilité dans l'implémentation SSL/TLS de Cisco Nexus Dashboard (CVE-2022-20860, score CVSS : 7,4) qui pourrait permettre à un attaquant distant non authentifié de modifier les communications avec les contrôleurs associés ou de visualiser des informations sensibles.

Bien qu'aucune des vulnérabilités susmentionnées ne soit censée être utilisée de manière malveillante dans des attaques réelles, il est absolument nécessaire que les utilisateurs des appareils concernés appliquent rapidement les correctifs.

Source : *https://bit.ly/3JaR2uZ*

Siemens

FortiGuard Labs découvre trois vulnérabilités dans les solutions de Siemens

18 Juillet 2022

Siemens et Open Design Alliance ont respectivement publié des correctifs pour résoudre trois vulnérabilités signalées par le chercheur de cybersécurité 'Yonghui Han' du FortiGuard Labs. Connues sous les noms de CVE-2022-28807, CVE-2022-28808 et CVE-2022-28809, les failles ont reçu un score de gravité importante. Toutes les trois ont une cause profonde liée au SDK Open Design Alliance Drawings qui affecte Siemens JT2Go et Teamcenter Visualization sous Windows par le biais de fichiers DWG. Elles pourraient permettre à un acteur de la menace de provoquer un plantage de l'application ou de divulguer des informations confidentielles.

Les failles sont des problèmes de corruption de mémoire existe dans le décodage des fichiers AutoCAD Drawing 'DWG' dans Open Design Alliance Drawings SDK. Plus précisément, elles sont causées par un fichier DWG malformé, qui provoque une lecture mémoire hors limites en raison d'une vérification de limites incorrecte.

Les attaquants peuvent exploiter ces vulnérabilités pour faire fuir des informations de mémoire dans le contexte de l'application via un fichier DWG modifié.

Il est recommandé aux utilisateurs d'appliquer les correctifs de Siemens dès que possible. En outre, Fortinet IPS protège les clients contre ces menaces zero day depuis leur découverte.

Source : *https://bit.ly/3JcM4hh*

Microsoft

Microsoft corrige des dizaines de bogues d'escalade de privilèges dans Azure Site Recovery

12 Juillet 2022

Microsoft a corrigé 32 vulnérabilités dans la suite Azure Site Recovery, dont deux permettent l'exécution de code à distance, et 30 vulnérabilités permettent une élévation de privilèges.

Dans un avis publié, Microsoft indique que les vulnérabilités d'injection SQL étaient la source de la plupart des bogues d'élévation de privilèges.

Cependant, Microsoft a également mis en évidence une vulnérabilité CVE-2022-33675 causée par une faille de détournement de DLL découverte par Tenable avec un indice de gravité CVSS v3 de 7,8.

Les attaques par détournement de DLL exploitent des vulnérabilités causées par des permissions non sécurisées sur les dossiers dans lesquels un système d'exploitation Windows recherche et charge les DLL nécessaires au lancement d'une application.

Pour mener à bien cette attaque, un pirate peut créer une DLL malveillante personnalisée utilisant le même nom qu'une DLL ordinaire chargée par l'application Azure Site Recovery. Cette dernière est ensuite stockée dans un dossier dans lequel Windows effectue des recherches, ce qui entraîne son chargement et son exécution au démarrage de l'application. Ensuite, en acquérant des privilèges d'administrateur sur un système cible, un attaquant serait libre d'administrer le système comme il souhait.

Pour résoudre tout problème de sécurité, veillez à appliquer les mises à jour de ce mois-ci.

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

SonicWall

SonicWall corrige une faille critique d'injection SQL

22 Juillet 2022

SonicWall a publié des mises à jour pour corriger une vulnérabilité critique de type injection SQL affectant les produits GMS (Global Management System) et Analytics On-Prem.

Suivie sous le nom de CVE-2022-22280 avec un score CVSS de 9.4, la faille permet à un acteur de la menace non authentifié d'effectuer une injection SQL en raison d'une mauvaise neutralisation des éléments spéciaux utilisés dans une commande SQL. Cette attaque ne nécessite pas une interaction avec l'utilisateur et sa complexité d'attaque est faible.

SonicWall précise qu'elle n'a connaissance d'aucun rapport d'exploitation active dans la nature ni de l'existence d'un exploit de type "proof of concept" (PoC) pour cette vulnérabilité.

En utilisant cette faille, les attaquants peuvent accéder à des données auxquelles ils ne devraient normalement pas avoir accès, contourner l'authentification ou éventuellement supprimer des données de la base de données.

En raison du déploiement généralisé de SonicWall GMS et Analytics, qui sont utilisés pour la gestion centrale, le déploiement rapide, la création de rapports en temps réel et l'analyse des données, la surface d'attaque est importante et concerne généralement des organisations critiques.

Actuellement, il n'y a pas de solution de contournement disponible pour cette vulnérabilité, il est donc recommandé de mettre à jour toutes les versions concernées vers GMS 9.3.1-SP2-Hotfix-2 et Analytics 2.5.0.3-Hotfix-1 ou des versions ultérieures afin d'atténuer tout risque possible.

Source : *https://bit.ly/3zb1wG9*

Zyxel

Les failles des pare-feu Zyxel rendent les réseaux d'entreprise ouverts aux attaques

22 Juillet 2022

Zyxel a publié des correctifs pour plusieurs de ses produits de pare-feu suite à la découverte de deux vulnérabilités de sécurité qui ont rendu les réseaux d'entreprise ouverts à l'exploitation.

La première, CVE-2022-2030, est une faille de type traversée de répertoire authentifié dans les programmes Common Gateway Interface (GLI) de certains pare-feu Zyxel. Elle est due à des séquences de caractères spécifiques dans une URL mal nettoyée.

La deuxième, CVE-2022-30526, est une vulnérabilité d'escalade de privilèges locaux (LPE) qui a été identifiée dans l'interface de ligne de commande (CLI) de certaines versions de pare-feu. Elle pourrait permettre à un attaquant local d'exécuter certaines commandes du système d'exploitation avec les privilèges de l'administrateur dans certains répertoires d'un dispositif vulnérable.

Ces bogues affectent différentes versions de plusieurs pare-feu Zyxel, notamment USG Flex, ATP Series, VPN Series et USG ZyWall.

Les correctifs sont actuellement disponibles, ce qui permet aux utilisateurs de les installer pour avoir une protection optimale.

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

Apple

Une dizaine de failles impactant les appareils Apple

20 Juillet 2022

Apple a publié des correctifs pour 37 failles de sécurité couvrant différents composants d'iOS et de macOS, elles pourraient permettre à un acteur de la menace d'effectuer plusieurs cyberattaques allant de l'élévation de privilèges à l'exécution de code arbitraire, en passant par la divulgation d'informations et le déni de service (DoS).

La principale d'entre elles est la CVE-2022-2294, une faille de corruption de mémoire dans le composant WebRTC que Google a révélée au début du mois comme ayant été exploitée dans des attaques réelles visant des utilisateurs du navigateur Chrome. Il n'y a cependant aucune preuve d'une exploitation de jour zéro de la faille dans la nature visant iOS, macOS et Safari.

En plus de CVE-2022-2294, les mises à jour corrigent également plusieurs failles d'exécution de code arbitraire ayant un impact sur Apple Neural Engine (CVE-2022-32810, CVE-2022-32829, et CVE-2022-32840), Audio (CVE-2022-32820), GPU Drivers (CVE-2022-32821), ImageIO (CVE-2022-32802), IOMobileFrameBuffer (CVE-2022-26768), Kernel (CVE-2022-32813 et CVE-2022-32815), et WebKit (CVE-2022-32792).

En outre, la dernière version de macOS résout cinq vulnérabilités de sécurité dans le module SMB qui pourraient permettre à une application malveillante d'obtenir des privilèges élevés, fuir des informations sensibles et exécuter du code arbitraire avec les privilèges du noyau.

Il est recommandé aux utilisateurs d'appareils Apple d'effectuer les dernières mises à jour des systèmes concernés afin de bénéficier des protections de sécurité les plus récentes.

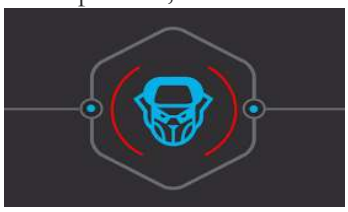
Source : *https://bit.ly/3cKwX2m*

Actualité

APT29 abuse des services de stockage en ligne Google Drive et Dropbox

Le groupe de Hacker APT29, exploitent désormais les services de cloud, notamment Google Drive et DropBox, dans leurs attaques pour abuser de la confiance des utilisateurs et éviter d'être détectés.

Le groupe a adopté cette nouvelle tactique dans ses récentes campagnes : une campagne a utilisé DropBox et, deux semaines plus tard, la deuxième campagne a utilisé Google Drive pour rester cachée.



Le groupe a utilisé Agenda[.]html pour désobfusquer une charge utile et pour écrire un fichier ISO malveillant sur le disque dur de la victime. Cette méthode est appelée HTML Smuggling.

De plus, des attaques de phishing ont ciblé des employés d'organisations diplomatiques dans le monde entier, contenant un lien vers un fichier HTML malveillant, EnvyScout qui est un dropper vers un malware secondaire, tel que Cobalt Strike.

EnvyScout peut être décrit comme un outil auxiliaire utilisé pour infecter davantage la cible avec l'implant de l'acteur. Il est utilisé pour désobscurcir le contenu du logiciel malveillant secondaire, qui est une ISO malveillante.

Le dropper EnvyScout est utilisé pour délivrer des charges utiles malveillantes supplémentaires, comme une balise Cobalt Strike.

La récente campagne d'APT29 témoigne de sa sophistication et de sa capacité à masquer le déploiement du malware. En outre, le groupe a réussi à abuser des services DropBox et Google Drive, qui sont très populaires auprès de millions de clients dans le monde. Leur inclusion dans le processus de diffusion des malwares d'APT est vraiment un problème sérieux.

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

Plusieurs nouvelles applications Play Store distribuent les malwares Joker, Facestealer et Coper

Google a pris des mesures pour éliminer du Play Store des dizaines d'applications frauduleuses qui ont été repérées comme propageant les familles de logiciels malveillants Joker, Facestealer et Coper.

Bien que la vitrine Android soit considérée comme une source fiable pour la découverte et l'installation d'applications, des acteurs malveillants ont trouvé à plusieurs reprises le moyen de passer outre les barrières de sécurité érigées par Google dans l'espoir d'inciter des utilisateurs peu méfiants à télécharger des applications contenant des logiciels malveillants.

Au total, 53 apps de téléchargement du Joker ont été identifiées par les deux entreprises de cybersécurité, les applications ayant été téléchargées cumulativement plus de 330 000 fois.

Il n'y a pas que Joker, puisque le chercheur en sécurité Maxime Ingrao a révélé huit applications contenant une variante différente du malware, appelée Autolycos, qui ont totalisé plus de trois millions de téléchargements avant d'être retirées.

"Ce qui est nouveau dans cette variante, c'est qu'elle ne nécessite plus de WebView", a déclaré le chercheur Pieter Arntz,. "Le fait de ne pas exiger de WebView réduit considérablement les chances que l'utilisateur d'un appareil affecté remarque que quelque chose de louche se passe. Autolycos évite le WebView en exécutant des URL sur un navigateur distant, puis en incluant le résultat dans les requêtes HTTP."

Des applications intégrant les malwares Facestealer et Coper ont également été découvertes sur la place de marché officielle. Alors que le premier permet aux opérateurs de siphonner les identifiants Facebook et les jetons d'authentification, Coper - un descendant du malware Exobot - fonctionne comme un cheval de Troie bancaire qui peut voler un large éventail de données.

Outre les règles de base habituelles en matière de téléchargement d'applications à partir des magasins d'applications, il est recommandé aux utilisateurs de ne pas accorder d'autorisations inutiles aux applications et de vérifier leur légitimité en vérifiant les informations relatives au développeur, en lisant les critiques et en examinant de près les politiques de confidentialité.

***Source :** https://bit.ly/3b9FSKm*

Les pirates peuvent usurper les métadonnées pour créer de faux dépôts GitHub

Les chercheurs en sécurité de Checkmarx ont mis en garde contre l'émergence d'une nouvelle tactique d'attaque de la chaîne d'approvisionnement impliquant des commits de métadonnées usurpées pour présenter des dépôts GitHub malveillants comme légitimes.

Selon les chercheurs, cette technique d'attaque permet aux acteurs de la menace de tromper les développeurs pour qu'ils utilisent du code malveillant. Dans le système de contrôle de version Git, les commits sont des éléments vitaux car ils enregistrent chaque modification apportée aux documents, la chronologie de la modification et l'auteur de la modification.

Ils ont constaté qu'un acteur menaçant pouvait falsifier les métadonnées de validation pour faire paraître un dépôt plus ancien qu'il ne l'est en réalité. Il peut également tromper les développeurs en présentant les dépôts comme fiables, car des contributeurs réputés les maintiennent. Il est également possible d'usurper l'identité du contributeur et d'attribuer la livraison à un compte GitHub authentique.

Les fausses métadonnées incitent les développeurs à utiliser du code qu'ils éviteraient autrement, et les acteurs de la menace gagnent en crédibilité. Pour prévenir l'attaque, les chercheurs de Checkmarx recommandent vivement aux développeurs de signer leurs commits et de toujours garder le mode vigilant activé sur les utilisateurs afin d'assurer une sécurité optimale de

l'écosystème du code. En mode vigilant, l'état de vérification de leurs commits est affiché, ce qui est une caractéristique convaincante contre l'attaque de la chaîne d'approvisionnement.

Source : *https://bit.ly/3PY9NUH*

Des attaquants utilisent des comptes PayPal pour usurper des marques populaires

Dans un billet de blog, les chercheurs d'Avanan ont déclaré qu'à partir de juin de cette année, ils ont vu des pirates utiliser PayPal pour envoyer des factures malveillantes et demander des paiements.

Les pirates envoient l'e-mail depuis le domaine de PayPal, en utilisant un compte PayPal gratuit auquel ils se sont inscrits, le corps de l'e-mail usurpant des marques comme Norton. Les pirates exploitent ensuite des sites Web légitimes et populaires pour pénétrer dans les boîtes de réception et voler des informations d'identification et de l'argent.

"Les utilisateurs doivent être informés de l'existence de ce type d'attaque et de la manière de la reconnaître", a déclaré M. Tiquet. "C'est le seul moyen de prévention, à part le filtrage et l'analyse de tous les e-mails qui semblent être une facture. La formation à la sensibilisation à la sécurité, pour être vraiment efficace, doit être continuellement mise à jour pour s'assurer que les utilisateurs sont au courant des dernières menaces."

Patrick Harr, directeur général de SlashNext, a déclaré que les entreprises doivent inclure des arnaques d'ingénierie sociale comme celles-ci dans les programmes de formation au phishing. Harr a déclaré que la main-d'œuvre hybride moderne utilise la technologie personnelle (apportez votre propre appareil, ou BYOD) et mobile, en particulier, car la plupart des entreprises n'ont pas tous les employés sur des appareils gérés.

Source : *https://bit.ly/3S6XWFL*

OrBit : un nouveau malware Linux très évasif

Un nouveau logiciel malveillant est utilisé pour voler silencieusement des informations sur des systèmes Linux protégés. Baptisé OrBit, le malware Linux est utilisé pour infecter tous les processus en cours sur les machines compromises.

Il peut accrocher différentes fonctions pour éviter la détection, maintenir la persistance en infectant de nouveaux processus, contrôler le comportement des processus et masquer l'activité du réseau.

Le malware peut gagner en persistance en utilisant deux techniques différentes pour empêcher les tentatives de suppression :

La première technique consiste à ajouter le chemin d'accès au logiciel malveillant dans le fichier de configuration /etc/ld[.]so[.]preload. Cela indique au chargeur que la porte dérobée doit être chargée en premier pour tous les nouveaux processus.

Dans la deuxième technique, le backdoor copie le binaire du chargeur afin de pouvoir le patcher. Il fait une simple recherche dans le binaire pour la chaîne "/etc/ld[.]so[.]preload".

Une fois trouvée, elle remplace la chaîne par un chemin d'accès à un fichier situé dans le %MALWARE_FOLDER%. Le contenu de ce fichier contient le chemin d'accès à la bibliothèque du logiciel malveillant pour agir comme un fichier de configuration de ld[.]so[.]preload.

Cela implique que, lorsqu'un chargeur de correctifs s'exécute, il utilise le fichier situé dans le %MALWARE_FOLDER% à la place de "/etc".

Ce malware doit donc être considéré comme une menace sérieuse pour les systèmes Linux. Il est recommandé de faire appel à des services de renseignement sur les menaces qui vous apportent des informations de première main pour identifier les nouveaux types de menaces et comprendre leur gravité. Les mesures d'atténuation peuvent être planifiées en conséquence.

Les mesures d'atténuation peuvent être planifiées en conséquence.

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

Les industries critiques échouent en matière de sécurité IIoT/OT

Selon un rapport de la société de sécurité Barracuda Networks, la plupart des entreprises de services critiques ont du mal à sécuriser leurs systèmes de l'internet industriel des objets (IIoT)/technologies opérationnelles (OT) et reconnaissent la nécessité d'investir plus massivement dans ces domaines.

L'entreprise a interrogé 800 responsables informatiques, responsables de la sécurité informatique et chefs de projet chargés des projets de sécurité IIoT/IoT dans un éventail d'industries, notamment l'agriculture, la biotechnologie, la construction, le gouvernement, la santé et la fabrication.

Le rapport a révélé que les entreprises rencontrent des problèmes lors de la mise en œuvre de projets de sécurité IIoT/OT, 93 % d'entre elles admettant avoir échoué. La principale cause d'échec est que la technologie a pris trop de temps à mettre en œuvre, tandis que les dépenses arrivent en deuxième position. Près de quatre entreprises sur dix ont également déclaré que personne dans l'organisation n'avait pris la responsabilité du projet.

Plus généralement, 94% des organisations ont connu un incident de sécurité au cours des 12 derniers mois. Près de neuf sur dix de celles qui ont subi un incident ont vu leurs opérations affectées pendant plus d'une journée, tandis que 23% ont été impactées pendant au moins trois jours.

Les applications Web ont été le vecteur d'attaque le plus important, à 42 %, suivies par l'utilisation de matériel externe malveillant ou de supports amovibles comme les clés USB, qui ont affecté 38 % des répondants.

Source : *https://bit.ly/3PWD1E1*

Bon à savoir

54% des PME ne disposent pas d'une solution MFA

Selon l'étude de Cyber Readiness Institute (CRI) sur l'authentification multifactorielle pour les petites entreprises, les PME du monde entier continuent de se reposer uniquement sur les noms d'utilisateur et les mots de passe pour sécuriser les données critiques.
La MFA est utilisée depuis des décennies et est largement recommandée par les experts en cybersécurité. Pourtant, 55 % des PME interrogées ne sont pas "très conscientes" de la MFA et de ses avantages en matière de sécurité, et 54 % ne l'utilisent pas pour leur entreprise. Parmi les entreprises qui n'ont pas mis en œuvre l'MFA, 47 % ont indiqué qu'elles ne comprenaient pas l'AMF ou n'en voyaient pas l'intérêt. En outre, près de 60 % des propriétaires de petites et moyennes entreprises n'ont pas discuté de la MFA avec leurs employés.
"Nous savons que presque toutes les attaques de compromission de comptes peuvent être stoppées nettes, simplement en utilisant le MFA. C'est un moyen efficace et éprouvé de contrecarrer les mauvais acteurs", a déclaré Karen S. Evans, directrice générale du CRI. "Nous tous - gouvernements, organisations à but non lucratif, industrie - devons faire beaucoup plus pour communiquer la valeur du MFA aux propriétaires de petites et moyennes entreprises."
La mise en œuvre de l'AMF ne nécessite pas de modifications matérielles des ordinateurs ou des appareils mobiles de l'entreprise. Au contraire, il existe de nombreux outils logiciels gratuits ou peu coûteux que les utilisateurs peuvent télécharger pour les utiliser dans leur entreprise et sur leurs appareils personnels.
Il est important d'utiliser un mot de passe fort, mais la complexité seule ne suffit pas, dont il est recommandé d'ajouter une deuxième couche de protection avec l'authentification multifactorielle pour une meilleure sécurisation de l'accès aux données confidentielles.

Source : *https://bit.ly/3Boh3Fa*

Evènements

Evènement du mois

Going Passwordless : The Future of Cybersecurity

28 Juillet 2022

Online

https://bit.ly/3vlCEuf

L'authentification sans mot de passe permet de renforcer la sécurité en éliminant les pratiques risquées de gestion des mots de passe et en réduisant les vecteurs d'attaque.
Dans ce webinaire, Michael Argast, cofondateur et PDG de Kobalt.io, va :

- Examiner l'évolution des mots de passe, les défis et les vulnérabilités ;
- Expliquer ce que signifie le "Passwordless" ;
- Explorer comment se présente un futur Passwordless ;
- Discuter des implications pour les utilisateurs finaux, les développeurs et la sécurité informatique ;
- Partager les meilleures pratiques de déploiement du cette technique pour répondre aux exigences de sécurité.

Evènement à venir

What are Deepfakes, and How Can We Detect Them ?

08 Août 2022

Online

https://bit.ly/3PWaVIm

Cet évènement a pour objectif d'expliquer ce que sont les « deepfakes » et comment utiliser les technologies d'IA/ML pour distinguer le vrai du faux, tout en abordant des exemples bien connus d'imitations profondes. Ce webcast couvrira les points suivants :

- La définition du deepfake ;
- Les façons permettant de confondre les ordinateurs et les gens ;
- La manière dont les empreintes numériques sont utilisées dans les algorithmes de détection ;
- Les défis à relever dans ce domaine.

Référence	ANPT-2022-BV-07
Titre	Bulletin de veille N°07
Date de version	31 Juillet 2022
Contact	ssi@anpt.dz