BULLETIN DE VEILLE N°06

ANPT-2024-BV-06

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

Juin 2024

Alertes de sécurité

Wget

Vulnérabilité critique CVE-2024-38428 dans wget

24 juin 2024

Il existe une vulnérabilité critique dans le programme en ligne de commande wget, qui a un score de base CVSS de 10.0. Le CERT-Bund signale cette vulnérabilité, qui est contenue dans les versions de wget <=1.24.5. Un attaquant peut mener une attaque non spécifiée. Toute personne utilisant wget sous Linux ou Windows doit prendre des mesures urgentes et cesser d'utiliser le programme. Il n'existe pas encore de version mise à jour.

La vulnérabilité affecte les versions open source de wget jusqu'à la version 1.24.5 incluse (qui est la version actuelle). Le CERT-Bund indique seulement qu'un attaquant anonyme à distance peut exploiter la vulnérabilité de wget pour mener une attaque non spécifiée. Cet avertissement de vulnérabilité est disponible sur GitHub.

CVE-2024-38428 signale que le module url.c de GNU Wget jusqu'à la version 1.24.5 gère incorrectement les points-virgules dans le sous-composant userinfo d'un URI. Cela peut conduire à un comportement dangereux où des données qui devraient être dans le sous-composant userinfo sont incorrectement interprétées comme faisant partie du sous-composant host

Les URL manipulés peuvent révéler des détails d'authentification et des informations sensibles. Il existe également un risque de manipulation. Norddeutsch l'a résumé comme L'Auth Details (exposition d'informations sensibles), manipulation de l'en-tête de l'hôte (hameçonnage, redirection MitM) et Fuite de données (exposition involontaire d'informations d'identification)

"Pour autant que je l'ai vu rapidement, il n'y a pas encore de mise à jour de wget qui corrige cette vulnérabilité. Vous devriez donc vous abstenir d'utiliser la ligne de commande pour le moment".

Source : https://bit.ly/3XL8ZtB

Vmware

VMware et Broadcom mettent en garde contre deux failles critiques dans vCenter, ainsi que contre un méchant bogue sudo

24 juin 2024

VMware by Broadcom a révélé une paire de failles classées critiques dans vCenter Server - l'outil utilisé pour gérer les machines virtuelles et les hôtes dans ses suites phares Cloud Foundation et vSphere.

Les failles classées critiques sont CVE-2024-37079 et CVE-2024-37080, qui obtiennent toutes deux un score de 9,8 sur l'échelle de dix points du système commun de notation des vulnérabilités (Common Vulnerability Scoring System v3).

Le bulletin de sécurité de VMware décrit ces deux failles comme des "vulnérabilités de débordement de tas dans l'implémentation du protocole DCE/RPC", ce qui signifie qu'un acteur malveillant disposant d'un accès réseau à vCenter Server peut déclencher ces vulnérabilités en envoyant un paquet réseau spécialement conçu, ce qui pourrait entraîner l'exécution de code à distance".

La bonne nouvelle est que des versions corrigées de vCenter Server et de Cloud Foundation sont déjà disponibles.

La mauvaise nouvelle est que VMware n'a pas examiné si les failles avaient un impact sur les anciennes versions de vSphere - ce qui signifie que les versions 6.5 et 6.7, dont le support a pris fin en octobre 2022 mais qui sont encore largement utilisées, peuvent être affectées mais ne seront pas corrigées.

VMware a également révélé une troisième faille - CVE-2024-37081 - décrite comme une "vulnérabilité locale d'élévation de privilèges due à une mauvaise configuration de sudo". Cette faille est classée importante, avec un score de 7.8, car elle pourrait signifier "Un utilisateur local authentifié avec des privilèges non administratifs peut exploiter ces problèmes pour élever ses privilèges à la racine sur vCenter Server Appliance"

Source : https://bit.ly/4d1ClZ9

Actualité

CoinStats affirme que des pirates nord-coréens ont pénétré dans 1 590 portefeuilles de crypto-monnaies

CoinStats a été victime d'une faille de sécurité massive qui a compromis 1 590 portefeuilles de crypto-monnaies, l'attaque étant soupçonnée d'avoir été menée par des acteurs nord-coréens.

CoinStats est une application complète de gestion de portefeuille de crypto-monnaies qui compte 1 500 000 utilisateurs. Elle est utilisée pour le suivi des investissements, les données en temps réel, l'agrégation de nouvelles et les alertes personnalisées. Elle permet également aux utilisateurs de créer des portefeuilles CoinStats, qui sont hébergés par la plateforme.

Pour les utilisateurs qui souhaitent utiliser les fonctions de gestion de portefeuille, la plateforme exige un accès en lecture seule aux portefeuilles cryptographiques externes connectés et n'ont pas été affectés par la brèche.

Toutefois, les utilisateurs qui hébergeaient leurs portefeuilles sur CoinStats ont potentiellement été touchés par le piratage.

Dans une annonce faite hier sur X, CoinStats a indiqué aux utilisateurs qu'ils avaient subi une cyberattaque qui avait affecté 1 590, soit 1,3 %, de tous les portefeuilles hébergés sur la plateforme.

La société a partagé une liste des portefeuilles touchés sur cette feuille de calcul, mais certains utilisateurs ont signalé que des fonds avaient été volés dans des portefeuilles qui ne figuraient pas sur cette liste. Par conséquent, l'ampleur réelle de l'incident pourrait être plus importante que ce que CoinStats a vérifié.

Les personnes dont l'adresse de portefeuille figure sur la liste et qui ont encore des fonds sont invitées à les transférer immédiatement vers un portefeuille externe.

Alors que le piratage est en cours, le site web et l'application CoinStats restent indisponibles pendant que l'entreprise enquête et atténue l'attaque.

L'attaque n'a pas eu d'impact sur les portefeuilles connectés et les échanges centralisés des utilisateurs, qui peuvent donc continuer à les utiliser en toute sécurité.

Bien que l'enquête soit en cours, le PDG de CoinStats a déclaré sur X qu'il détenait des preuves significatives suggérant que des pirates nord-coréens avaient mené l'attaque, partageant un document CISA sur le groupe de pirates nord-coréens Lazarus.

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

Le cyberespionnage chinois cible les opérateurs de télécommunications en Asie depuis 2021

Des groupes de cyberespionnage associés à la Chine ont été liés à une campagne de longue haleine qui a infiltré plusieurs opérateurs de télécommunications situés dans un seul pays asiatique au moins depuis 2021.

"Les attaquants ont placé des portes dérobées sur les réseaux des entreprises ciblées et ont également tenté de voler des informations d'identification", a déclaré l'équipe Symantec Threat Hunter, qui fait partie de Broadcom, dans un rapport partagé avec The Hacker News.

L'entreprise de cybersécurité n'a pas révélé le pays ciblé, mais a déclaré avoir trouvé des preuves suggérant que la cyberactivité malveillante pourrait avoir commencé dès 2020.

Les attaques ont également visé une société de services anonyme du secteur des télécommunications et une université d'un autre pays asiatique.

Le choix des outils utilisés dans cette campagne recoupe d'autres missions menées par des groupes d'espionnage chinois tels que Mustang Panda, RedFoxtrot et Naikon au cours des dernières années.

Il s'agit notamment de portes dérobées personnalisées, telles que COOLCLIENT, QUICKHEAL et RainyDay, qui permettent de capturer des données sensibles et d'établir une communication avec un serveur de commande et de contrôle (C2).

Bien que la voie d'accès initiale exacte utilisée pour atteindre les cibles soit actuellement inconnue, la campagne se distingue également par le déploiement d'outils de balayage de ports et le vol d'informations d'identification par le biais de l'extraction de ruches du registre Windows.

Le fait que les outils soient connectés à trois collectifs d'adversaires différents a soulevé plusieurs possibilités : Les attaques sont menées indépendamment les unes des autres, un seul acteur de la menace utilise des outils acquis auprès d'autres groupes, ou divers acteurs collaborent à une même campagne.

À ce stade, on ne sait pas non plus quel est le motif principal de ces intrusions, bien que les acteurs chinois aient l'habitude de s'en prendre au secteur des télécommunications dans le monde entier.

Source : https://bit.ly/3W33wNq

Bon à savoir

La connexion 5G de votre téléphone est vulnérable aux contournements et aux attaques DoS

Les appareils mobiles sont exposés à des risques de vol de données et de déni de service gratuits, grâce aux vulnérabilités des technologies 5G.

Lors de la prochaine édition de Black Hat 2024 à Las Vegas, une équipe de sept chercheurs de la Penn State University décrira

comment les pirates peuvent aller au-delà du sniffing de votre trafic Internet en vous fournissant littéralement votre connexion Internet. À partir de là, l'espionnage, l'hameçonnage et bien d'autres choses encore sont possibles.
Selon eux, il s'agit d'une forme d'attaque remarquablement accessible, qui fait appel à des vulnérabilités souvent négligées et à du matériel que l'on peut acheter en ligne pour quelques centaines de dollars.
La première chose à faire est de Configurer une fausse station de base à laquelle les téléphones peuvent se connecter, Lorsqu'un appareil tente pour la première fois de se connecter à une station de base d'un réseau mobile, les deux tentatives font l'objet d'une authentification et d'un accord de clé (AKA). L'appareil envoie une demande d'enregistrement et la station répond par des demandes d'authentification et des contrôles de sécurité
Après avoir attiré un appareil ciblé, un attaquant peut utiliser ce contournement AKA pour renvoyer un message "d'acceptation de l'enregistrement" malicieusement conçu et établir une connexion. À ce stade, le pirate devient le fournisseur d'accès à Internet de la victime, capable de voir tout ce qu'elle fait sur le Web en clair. Il peut également attirer l'attention de la victime en lui envoyant, par exemple, un message SMS de spear phishing ou en la redirigeant vers des sites malveillants.
Bien que le contournement de l'AKA soit le plus grave, les chercheurs ont découvert d'autres vulnérabilités qui leur permettraient de déterminer l'emplacement d'un appareil et de procéder à un déni de service.

Evènements

Evènement à venir

Pittsburgh CyberSecurity Conference 2024
11 juin 2024 – Online
https://bit.ly/3RMpy4o

La conférence de Pittsburgh sur la cybersécurité s'adresse aux professionnels de haut niveau travaillant dans la communauté de la sécurité ; elle s'efforce de rassembler les meilleurs esprits du secteur pour leur faire vivre une expérience unique en matière de cybersécurité. Elle propose des présentations stimulantes par des leaders de l'industrie de la sécurité, des conférenciers d'honneur estimés et une discussion en panel avec des professionnels expérimentés et une équipe talentueuse qui sont à l'avant-garde des stratégies de pointe pour la défense de la cybersécurité.

Référence	ANPT-2024-BV-06
Titre	Bulletin de veille N°06
Date de version	30 juin 2024
Contact	ssi@anpt.dz