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

BULLETIN DE VEILLE N°05

ANPT-2024-BV-05

Mai 2024

Alertes de sécurité

GitHub

Une vulnérabilité critique de Git permet un RCE lors du clonage de dépôts avec des sous-modules (CVE-2024-32002).

16 Mai 2024

De nouvelles versions de Git sont disponibles, avec des correctifs pour cinq vulnérabilités, dont la plus critique (CVE-2024-32002). Il s'agit d'une vulnérabilité critique qui permet à des dépôts Git spécialement conçus avec des sous-modules de tromper Git en écrivant des fichiers dans un répertoire .git/ au lieu de l'arborescence du sous-module.

« Cela est possible en confondant Git avec un répertoire et un lien symbolique qui ne diffèrent que par la casse, de sorte que Git peut écrire soit l'un, soit l'autre, mais pas les deux. Cette confusion peut être utilisée pour manipuler Git et lui faire écrire un hook qui sera exécuté alors que l'opération de clonage est toujours en cours, ne donnant à l'utilisateur aucune possibilité d'inspecter le code qui est exécuté", a expliqué Johannes Schindelin, responsable de Git pour Windows.

La CVE-2024-32004 permet également l'exécution de code à distance, mais uniquement sur les machines multi-utilisateurs : « Un attaquant peut préparer un dépôt local de manière à ce qu'il ressemble à un clone partiel auquel il manque un objet, de sorte que, lorsque ce dépôt est cloné, Git exécute un code arbitraire pendant l'opération avec toutes les permissions de l'utilisateur effectuant le clonage. »

CVE-2024-32465 peut permettre à des attaquants de contourner les protections pour le clonage de dépôts non fiables, CVE-2024-32020 peut permettre à des utilisateurs non fiables de modifier des objets dans le dépôt cloné (local), et CVE-2024-32021 peut être utilisé pour manipuler Git afin d'écrire des fichiers en dehors de l'arbre de travail Git et en dehors du répertoire .git/.

Les vulnérabilités ont été corrigées dans Git v2.45.1, v2.44.1, v2.43.4, v2.42.2, v2.41.1, v2.40.2 et v2.39.4.

Il a également indiqué que d'autres modifications avaient été apportées à Git pour rendre le processus de clonage plus sûr : améliorations de la protection contre l'exécution de code à distance, meilleure gestion des liens symboliques et des répertoires, moyen plus sûr d'exécuter des hooks (scripts), et bien d'autres choses encore.

Source : https://bit.ly/3X9olaG

Cisco

Une vulnérabilité de haute gravité affecte le centre de gestion Cisco Firepower

27 Mai 2024

Cisco a corrigé une vulnérabilité, répertoriée comme CVE-2024-20360 (CVSS score 8.8), dans l'interface de gestion basée sur le web du logiciel Firepower Management Center (FMC).

La vulnérabilité est un problème d'injection SQL, un attaquant peut exploiter la faille pour obtenir n'importe quelle donnée de la base de données, exécuter des commandes arbitraires sur le système d'exploitation sous-jacent, et élever les privilèges à root. L'attaquant ne peut exploiter cette vulnérabilité que s'il dispose au moins d'informations d'identification en lecture seule.

« Une vulnérabilité dans l'interface de gestion basée sur le web du logiciel Cisco Firepower Management Center (FMC) pourrait permettre à un attaquant distant authentifié de mener des attaques par injection SQL sur un système affecté », peut-on lire dans l'avis.

« Cette vulnérabilité existe parce que l'interface de gestion basée sur le web ne valide pas de manière adéquate les entrées de l'utilisateur. Un pirate peut exploiter cette vulnérabilité en s'authentifiant auprès de l'application et en envoyant des requêtes SQL élaborées à un système affecté. Une exploitation réussie pourrait permettre à l'attaquant d'obtenir n'importe quelle donnée de la base de données, d'exécuter des commandes arbitraires sur le système d'exploitation sous-jacent et d'élever ses privilèges au niveau de root. Pour exploiter cette vulnérabilité, un attaquant doit au moins disposer d'informations d'identification en lecture seule ».

Cisco déclare qu'il n'existe pas de solution de contournement pour remédier à cette vulnérabilité. Le géant de l'informatique a confirmé que cette vulnérabilité n'affecte pas le logiciel Adaptive Security Appliance (ASA) ni le logiciel Firepower Threat Defense (FTD).

L'équipe Cisco Product Security Incident Response Team (PSIRT) n'a pas connaissance d'attaques dans la nature exploitant cette vulnérabilité.

*Source :*https://bit.ly/3Vw8rq1

Actualité

Des pirates informatiques chinois se cachent sur des réseaux militaires et gouvernementaux depuis 6 ans

Baptisé Unfading Sea Haze (PDF), axé sur l'espionnage et capable de regagner l'accès aux environnements compromis, le groupe de pirates informatiques est resté sous le radar depuis 2018 en utilisant des outils, tactiques et techniques (TTP) nouveaux et améliorés.

Bien que le vecteur d'intrusion initial employé par Unfading Sea Haze ne soit pas connu, l'acteur de la menace a été observé en train d'employer le spear-phishing dans certaines attaques, suivi par le déploiement de logiciels malveillants et d'outils personnalisés.

Les courriels de spear-phishing utilisés dans les attaques de l'année dernière comprenaient des archives malveillantes contenant des fichiers LNK conçus pour exécuter des commandes malveillantes à la place, ce qui a conduit au déploiement de logiciels malveillants.

Pour persister, Unfading Sea Haze a utilisé des tâches planifiées associées à la manipulation de comptes d'administrateurs locaux. Les attaquants ont tenté d'activer/désactiver les comptes d'administrateur, de réinitialiser son mot de passe et de le masquer de l'écran de connexion.

En outre, l'acteur de la menace a été observé en train d'utiliser des outils de surveillance et de gestion à distance (RMM) disponibles dans le commerce, tels que ITarian RMM, pour accéder aux réseaux des victimes.

« Nous avons également trouvé des preuves suggérant que l'attaquant a pu établir une persistance sur les serveurs web, y compris Windows IIS et Apache httpd. Les méthodes potentielles incluent des shells web ou des modules malveillants conçus pour ces plateformes de serveurs web (modules IIS et modules httpd)", note Bitdefender.

Entre 2018 et 2023, Unfading Sea Haze s'est appuyé sur deux variantes de RAT Gh0st nommées SilentGh0st et TranslucentGh0st, et sur des variantes de l'agent .NET SharpJSHandler, qui était pris en charge par un chargeur nommé Ps2dllLoader pour exécuter des charges utiles en mémoire.

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

Des pirates informatiques exploitent des organismes financiers à l'aide d'un clone trojanisé

Des pirates utilisent le code d'un clone Python du vénérable jeu Minesweeper de Microsoft pour dissimuler des scripts malveillants dans des attaques contre des organisations financières européennes et américaines.

Le CSIRT-NBU et le CERT-UA d'Ukraine attribuent les attaques à un acteur de la menace identifié sous le nom de « UAC-0188 », qui utilise le code légitime pour dissimuler des scripts Python qui téléchargent et installent SuperOps RMM.

Superops RMM est un logiciel légitime de gestion à distance qui donne aux acteurs distants un accès direct aux systèmes compromis.

L'attaque commence par un courriel envoyé à partir de l'adresse « support@patient-docs-mail.com », usurpant l'identité d'un centre médical et ayant pour objet « Personal Web Archive of Medical Documents.

Le destinataire est invité à télécharger un fichier .SCR de 33 Mo à partir du lien Dropbox fourni. Ce fichier contient un code inoffensif provenant d'un clone Python du jeu Minesweeper ainsi qu'un code Python malveillant qui télécharge des scripts supplémentaires à partir d'une source distante (« anotepad.com »).

L'inclusion du code du jeu Minesweeper dans l'exécutable sert de couverture à la chaîne de 28 Mo codée en base64 contenant le code malveillant, dans le but de le faire apparaître comme inoffensif aux yeux des logiciels de sécurité.

En outre, le code Minesweeper contient une fonction nommée « create_license_ver » qui est réutilisée pour décoder et exécuter le code malveillant caché, de sorte que des composants logiciels légitimes sont utilisés pour masquer et faciliter la cyberattaque.

La chaîne base64 est décodée pour assembler un fichier ZIP contenant un programme d'installation MSI pour SuperOps RMM, qui est ensuite extrait et exécuté à l'aide d'un mot de passe statique.

SuperOps RMM est un outil légitime d'accès à distance, mais dans ce cas, il est utilisé pour accorder aux attaquants un accès non autorisé à l'ordinateur de la victime.

Le CERT-UA note que les organisations qui n'utilisent pas le produit SuperOps RMM doivent considérer sa présence ou l'activité réseau associée, comme les appels aux domaines « superops.com » ou « superops.ai », comme un signe de compromission de la part des pirates. L'agence a également partagé d'autres indicateurs de compromission (IoC) associés à cette attaque au bas du rapport.

Source : https://bit.ly/4bPJNG2

Bon à savoir

Les Bonnes pratiques lors de la navigation sur internet

En matière de cybersécurité lors de la navigation sur l'internet, plusieurs pratiques clés peuvent améliorer de manière significative votre sécurité en ligne.

- Tout d'abord, veillez à ce que votre navigateur soit toujours mis à jour pour bénéficier des correctifs de sécurité.
- Veillez à visiter des sites web compatibles HTTPS pour crypter vos données lors de la transmission.
- Utilisez des mots de passe forts et uniques pour chaque site et envisagez d'utiliser un gestionnaire de mots de passe réputé pour une meilleure gestion. Activez l'authentification multifactorielle chaque fois que possible pour ajouter

une couche de sécurité supplémentaire.

- Soyez prudent lors de l'installation de plugins et d'extensions, ne choisissez que ceux qui proviennent de sources fiables et vérifiez régulièrement s'ils sont nécessaires.
- Utilisez des logiciels antivirus et anti-malware fiables pour détecter et bloquer les activités malveillantes. Effacez régulièrement les cookies et le cache de votre navigateur pour empêcher le suivi et réduire le risque de vol de données.
- Évitez d'enregistrer vos mots de passe directement dans le navigateur et optez plutôt pour un gestionnaire de mots de passe spécialisé.
- Utilisez le mode de navigation privée, en particulier sur les ordinateurs partagés ou publics, pour éviter de stocker l'historique de navigation et les données personnelles.
- Ajustez les paramètres de confidentialité de votre navigateur pour limiter la collecte de données et le suivi par des tiers. Soyez vigilant en ce qui concerne les téléchargements, n'obtenez des fichiers qu'à partir de sources fiables et vérifiez leur authenticité. Méfiez-vous des escroqueries par hameçonnage et ne fournissez jamais d'informations personnelles en réponse à des demandes non sollicitées.
- Déconnectez-vous de vos comptes après utilisation, en particulier sur des appareils partagés ou publics, afin d'éviter tout accès non autorisé.
- Envisagez d'utiliser les fonctions de sandboxing du navigateur pour isoler les activités de navigation du reste de votre système pour plus de sécurité. Enfin, restez informé des nouvelles menaces et des meilleures pratiques en matière de cybersécurité afin de maintenir une approche proactive de la sécurité en ligne.

Evènements

Evènement à venir

Cyberconférence de Chatham House 2024

05 juin - online

https://bit.ly/4d9tYeF

La Chatham House Cyber Conference se concentre sur les avancées technologiques, les menaces et les opportunités dans le cyberespace. L'événement comprend des tables rondes, des sessions exclusives sur la règle de Chatham House et des opportunités de réseautage pour les décideurs politiques et les experts en cybersécurité afin de discuter de l'agilité dans un paysage cybernétique complexe. Rejoignez-nous pour découvrir des perspectives innovantes et renforcer vos stratégies de cybersécurité.

Référence	ANPT-2024-BV-05
Titre	Bulletin de veille N°05
Date de version	30 Mai 2024
Contact	ssi@anpt.dz