"Cybercrime is the greatest threat to every company in the world."
— Ginni Rometty

BULLETIN DE VEILLE N°12

ANPT-2024-BV-12

Décembre 2024

Alertes de sécurité

Apache

CVE-2024-45387 (CVSS 9.9) : Vulnérabilité critique d'injection SQL trouvée dans Apache Traffic Control

25 Novembre 2024

Une faille de sécurité de gravité critique a été découverte dans Apache Traffic Control, une plateforme open-source populaire utilisée pour construire des réseaux de diffusion de contenu (CDN) à grande échelle. Cette vulnérabilité, identifiée sous le nom de CVE-2024-45387 et dotée d'un score CVSS de 9.9, pourrait permettre à des attaquants d'exécuter un code SQL malveillant, ce qui pourrait compromettre des données sensibles et perturber des services critiques.

Apache Traffic Control est une plateforme hautement distribuée et évolutive qui aide les opérateurs à mettre en place des CDN robustes. Construite autour d'Apache Traffic Server, elle assure la diffusion efficace de contenus à grande échelle, en répondant aux besoins des opérateurs, qu'ils soient petits ou grands. Les composants clés de Traffic Control comprennent Traffic Ops, qui gère la configuration et les interactions du CDN.

La vulnérabilité provient d'une faiblesse d'injection SQL dans le composant Traffic Ops des versions 8.0.0 et 8.0.1 d'Apache Traffic Control. « Une vulnérabilité d'injection SQL dans Traffic Ops... permet à un utilisateur privilégié ayant le rôle 'admin', 'federation', 'operations', 'portal', ou 'steering' d'exécuter un code SQL arbitraire contre la base de données en envoyant une requête PUT spécialement conçue », explique le rapport officiel sur la vulnérabilité.

Cela signifie que des acteurs malveillants disposant de certains accès privilégiés à Traffic Ops pourraient exploiter cette faille pour manipuler la base de données sous-jacente. Les conséquences peuvent aller de la violation de données et de l'accès non autorisé à la prise de contrôle complète du système.

La vulnérabilité CVE-2024-45387 a été découverte par Yuan Luo du Tencent YunDing Security Lab et a été corrigée dans la version 8.0.2 d'Apache Traffic Control.

Les organisations utilisant Apache Traffic Control sont fortement encouragées à mettre à jour immédiatement vers la dernière version. Il est recommandé aux utilisateurs de passer à la version 8.0.2 d'Apache Traffic Control s'ils utilisent une version affectée de Traffic Ops.

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

Sophos

Sophos publie une mise à jour urgente de la sécurité des pares-feux

27 Novembre 2024

Sophos a annoncé la résolution de trois vulnérabilités de sécurité critiques affectant son produit Sophos Firewall, un outil de sécurité réseau largement utilisé. Ces vulnérabilités présentent des risques importants, notamment l'exécution de code à distance et l'élévation de privilèges.

CVE-2024-12727 : Injection SQL avant l'authentification (CVSS 9.8) : L'une des failles les plus critiques, CVE-2024-12727, est une vulnérabilité d'injection SQL avant authentification dans la fonction de protection du courrier électronique de Sophos Firewall. Si elle est exploitée, cette vulnérabilité peut permettre à des attaquants d'accéder à la base de données de reporting et d'exécuter du code à distance dans des conditions spécifiques. Ces conditions incluent l'activation de la fonction Secure PDF eXchange (SPX) et le fonctionnement du pare-feu en mode Haute Disponibilité (HA). Sophos note : « Le problème, qui affecte environ 0,05% des appareils, a été découvert et divulgué de manière responsable à Sophos par un chercheur en sécurité externe via le programme Sophos bug bounty. »

CVE-2024-12728 : Phrase de passe SSH non sécurisée (CVSS 9.8) Elle implique la réutilisation d'une phrase de passe SSH suggérée et non aléatoire après le processus d'établissement de l'AH. Cette négligence pourrait exposer des comptes système privilégiés sur les appareils concernés si SSH est activé. Sophos estime qu'environ 0,5% des appareils sont à risque.

La troisième vulnérabilité, CVE-2024-12729, permet aux utilisateurs authentifiés d'exécuter un code arbitraire via le portail utilisateur. Un chercheur externe a également divulgué ce problème à Sophos de manière responsable. Bien qu'il nécessite une authentification, il représente toujours un risque important pour les organisations qui s'appuient sur Sophos Firewall pour leur sécurité.

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

Actualité

Les systèmes électoraux roumains ont été la cible de plus de 85 000 cyberattaques

Un rapport déclassifié du service de renseignement roumain indique que l'infrastructure électorale du pays a été la cible de plus de 85 000 cyberattaques. Des acteurs menaçants ont également obtenu des identifiants d'accès à des sites web liés aux élections et les ont divulgués sur un forum de pirates russes moins d'une semaine avant le premier tour de l'élection présidentielle.

Le Service roumain de renseignement (SRI) indique que le 19 novembre, l'infrastructure informatique de l'Autorité électorale permanente (AEP) du pays a été la cible d'une cyberattaque qui a compromis un serveur contenant des données cartographiques qui était connecté à la fois au web public et au réseau interne de l'AEP.

À la suite de cet incident, les identifiants des sites électoraux roumains, notamment bec.ro (Bureau central des élections), roaep.ro et registrulelectoral.ro (inscription des électeurs), ont fait l'objet d'une fuite sur un forum russe de cybercriminalité.

Selon le SRI, l'attaquant a obtenu les identifiants en ciblant des utilisateurs légitimes ou en exploitant des vulnérabilités dans le serveur de formation des opérateurs des sections de vote.

Bien que le SRI n'attribue pas ces attaques à un acteur spécifique, l'agence estime que le modus operandi et les ressources nécessaires à l'activité pointent vers un acteur étatique. Dans un autre rapport déclassifié, le SRI décrit une campagne d'influence visant l'élection présidentielle roumaine, où plus de 100 influenceurs roumains de TikTok avec plus de 8 millions de followers actifs ont été manipulés pour distribuer du contenu électoral promouvant le candidat présidentiel Calin Georgescu.

Les influenceurs ont reçu des montants à partir de 100 $ pour 20 000 followers, pour diffuser des vidéos avec des hashtags décrivant le profil présidentiel de Georgescu.

Le ministère roumain de l'intérieur (MAI) affirme que la visibilité de ces vidéos a fortement augmenté à partir du 13 novembre et a culminé à la 9e place du top trending content, avec des centaines de millions de vues le 26 novembre.

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

Une organisation américaine en Chine est la cible d'attaquants

Une grande organisation américaine ayant une présence importante en Chine a fait l'objet d'une attaque ciblée au début de l'année, au cours de laquelle les attaquants ont obtenu une présence persistante sur son réseau, apparemment dans le but de collecter des renseignements. L'attaque a probablement été menée par un acteur de la menace basé en Chine, puisque certains des outils utilisés dans cette attaque ont été précédemment associés à des attaquants chinois. Bien qu'il soit possible que l'intrusion dans le réseau ait eu lieu plus tôt, les premières preuves de l'activité de l'attaquant datent d'avril 2024, et cette activité malveillante s'est poursuivie jusqu'en août 2024. Les attaquants se sont déplacés latéralement sur le réseau de l'organisation, compromettant plusieurs ordinateurs. Certaines des machines ciblées étaient des serveurs Exchange, ce qui laisse supposer que les attaquants recueillaient des renseignements en récoltant des courriels. Des outils d'exfiltration ont également été déployés, ce qui laisse supposer que des données ciblées ont été extraites des organisations.

Les preuves disponibles suggèrent que l'organisation a été violée par un acteur basé en Chine. Outre le fait que le sideloading de DLL est une tactique largement privilégiée par les groupes chinois, la même organisation a été ciblée en 2023 par un attaquant ayant des liens provisoires avec le groupe Daggerfly basé en Chine.

Sophos et RecordedFuture ont précédemment signalé que le fichier textinputhost.dat avait été utilisé par le groupe d'espionnage Crimson Palace, basé en Chine, dans le cadre d'attaques contre l'Asie du Sud-Est. Dans ce cas, il était utilisé en conjonction avec un exécutable nommé rc.exe. Le même nom de fichier a également été utilisé par les attaquants qui ont mené cette attaque.

Les technologies de sécurité comportementale de Symantec Endpoint Security offrent à nos clients une protection contre les attaques sans fichier, les attaques « Living Off the Land » et les attaques basées sur le comportement, y compris les activités de ligne de commande atypiques et les comportements d'application suspects tels que les exécutables sans processus ou le chargement latéral de DLL.

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

Bon à savoir

Pourquoi il faut limiter le partage d'informations personnelles

Le limiter de partage d'informations personnelles est essentiel pour protéger votre vie privée et maintenir la sécurité en ligne dans un monde de plus en plus numérique. Un partage excessif peut vous exposer à des risques tels que l'usurpation d'identité, la fraude, les attaques par hameçonnage ou l'ingénierie sociale. De nombreux attaquants s'appuient sur des informations accessibles au public pour concevoir des escroqueries personnalisées ou obtenir un accès non autorisé à vos comptes. Évitez de communiquer des informations sensibles telles que votre adresse, votre numéro de téléphone, votre numéro de sécurité sociale ou des informations financières sur les médias sociaux ou toute autre plateforme publique. Même des messages apparemment anodins, comme l'annonce de vacances ou le partage d'une photo de famille, peuvent fournir des indices sur des menaces potentielles. Passez en revue et réglez les paramètres de confidentialité de vos comptes de médias sociaux afin de limiter les personnes qui peuvent voir vos messages et vos données personnelles. Limitez l'utilisation de votre vrai nom, de votre date de naissance ou de votre titre professionnel sur les forums publics, et envisagez d'utiliser des alias ou des pseudonymes pour les comptes qui ne nécessitent pas de vérification.

Les photos doivent être partagées avec prudence, car elles peuvent révéler par inadvertance des informations privées par le biais d'objets visibles ou de métadonnées, telles que des balises de localisation. Évitez de saisir des informations personnelles sur des sites web lorsque vous utilisez des réseaux Wi-Fi publics, car ceux-ci sont souvent peu sûrs et vulnérables à l'interception des données. Soyez sceptique à l'égard des services en ligne, des applications ou des concours qui demandent des informations personnelles excessives sans raison claire et valable. Au lieu de cela, ne partagez que ce qui est strictement nécessaire et assurez-vous que le service est digne de confiance. Surveillez régulièrement votre empreinte numérique pour savoir quelles informations vous concernant sont accessibles au public et prenez des mesures pour les supprimer ou les sécuriser. En vous informant sur les tactiques d'ingénierie sociale, vous pouvez reconnaître si quelqu'un essaie d'exploiter vos informations personnelles. En prenant ces précautions, vous réduisez votre exposition aux cybermenaces et gardez un meilleur contrôle sur votre identité numérique, ce qui vous assure à la fois sécurité et tranquillité d'esprit.

Evènements

Evènement à venir

International Conference on Cybersecurity Studies (ICCSTUD-2025)

06 jan 2025

Sétif, Algérie

https://bit.ly/3BZuhef

The International Society for Engineering Research (ISER) is dedicated to creating a global platform for researchers and academicians to exchange knowledge and ideas. Its conferences foster collaboration across science and technology, encouraging interdisciplinary innovation to address global challenges. ISER emphasizes networking, mentorship, and partnerships, bridging gaps between academia and industry. By nurturing new ideas, it aims to drive advancements with tangible societal impacts. ISER's vision is to build a connected research ecosystem for sustainable development and progress.

Référence	ANPT-2024-BV-12
Titre	Bulletin de veille N°12
Date de version	31 Décembre 2024
Contact	ssi@anpt.dz