BULLETIN DE VEILLE N°10

ANPT-2024-BV-10

"The human factor is the weakest link in cybersecurity.."
— Bruce Schneier

Octobre 2024

Alertes de sécurité

Samsung

Les chercheurs du Threat Analysis Group (TAG) de Google mettent en garde contre une vulnérabilité zero-day de Samsung qui est largement exploitée.

25 octobre 2024

Le groupe d'analyse des menaces (TAG) de Google met en garde contre une vulnérabilité zero-day de Samsung, répertoriée sous le nom de CVE-2024-44068 (score CVSS de 8,1), qui est largement exploitée

La vulnérabilité est un problème de type « use-after-free », les attaquants pourraient exploiter la faille pour escalader les privilèges sur un appareil Android vulnérable.

Une vulnérabilité réside dans les processeurs mobiles de Samsung et, selon les experts, elle a été associée à d'autres vulnérabilités pour permettre l'exécution d'un code arbitraire sur les appareils vulnérables.

Samsung a corrigé la vulnérabilité en publiant des mises à jour de sécurité en octobre 2024.

« Un Use-After-Free dans le processeur mobile conduit à une escalade des privilèges » , peut-on lire dans l'avis publié par le conglomérat multinational coréen.

L'entreprise n'a pas confirmé que la vulnérabilité est activement exploitée dans la nature.

Les versions concernées sont les Exynos 9820, 9825, 980, 990, 850 et W920.

La vulnérabilité a été découverte par les chercheurs Xingyu Jin de Google Devices & Services Security Research et Clement Lecigene de Google Threat Analysis Group.

Les chercheurs de Google ont rapporté que la vulnérabilité réside dans un pilote qui fournit une accélération matérielle pour des fonctions multimédias telles que le décodage JPEG et l'affichage d'images.

Le fait que Google TAG ait découvert la faille suggère que les vendeurs de logiciels espions commerciaux ont pu utiliser l'exploit pour cibler les appareils Samsung.

L'avis publié par Google Project Zero met en garde contre la disponibilité d'un exploit de type « zero-day » qui fait partie d'une chaîne d'élévation de privilèges.

Source : ***https://bit.ly/4fx88Cl***

Redhat

Red Hat met en garde contre la faille d'escalade de privilèges CVE-2024-9050 dans NetworkManager-libreswan

22 Septembre 2024

Une vulnérabilité récemment découverte dans le plugin client libreswan pour NetworkManager pourrait permettre aux attaquants d'obtenir un accès root sur les systèmes Red Hat Enterprise Linux 9.

Red Hat a publié un avis de sécurité signalant une vulnérabilité de haute sévérité (CVE-2024-9050) dans le paquetage NetworkManager-libreswan. Cette faille pourrait permettre à un attaquant local d'élever ses privilèges et d'exécuter du code arbitraire avec les privilèges de l'administrateur.

La vulnérabilité provient d'une mauvaise analyse des configurations VPN. « Dans cette configuration, composée d'un format clé-valeur, le plugin n'échappe pas aux caractères spéciaux, ce qui conduit l'application à interpréter les valeurs comme des clés », explique le bulletin de sécurité de Red Hat. Cela permet à un pirate de manipuler le paramètre leftupdownkey, qui exécute une commande en tant que rappel. En injectant des commandes malveillantes, un pirate peut contourner les mesures de sécurité et prendre le contrôle complet du système.

« Ce problème est marqué d'une gravité importante en raison de son potentiel à permettre l'escalade des privilèges locaux et l'exécution de code arbitraire », indique Red Hat.

La vulnérabilité est particulièrement préoccupante car NetworkManager utilise Polkit pour permettre aux utilisateurs non privilégiés de gérer les paramètres du réseau. Ce mécanisme, destiné à faciliter la tâche de l'utilisateur, fournit par inadvertance un vecteur d'attaque permettant d'exploiter cette faille. Red Hat a corrigé la CVE-2024-9050 dans Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions. Les utilisateurs sont invités à mettre à jour leurs systèmes immédiatement.

Source : ***https://bit.ly/40AIc4q***

Actualité

La plateforme de crypto-monnaies Radiant Capital déclare que 50 millions de dollars en pièces numériques ont été volés à la suite de la compromission de comptes.

Plus de 50 millions de dollars de crypto-monnaies ont été volés à la plateforme financière décentralisée Radiant Capital mercredi soir.

Dans un rapport post-mortem publié jeudi, Radiant a déclaré que l'attaque a compromis trois développeurs, qui sont tous des contributeurs de longue date et de confiance de la plateforme. La société s'est présentée comme un marché monétaire « à guichet unique » où les utilisateurs peuvent déposer et emprunter des crypto-monnaies sur différentes blockchains. Plusieurs experts en sécurité ont déclaré sur les médias sociaux que le pirate a eu accès à plusieurs clés privées appartenant à des développeurs de l'entreprise, ce qui a permis à l'acteur de la menace de drainer les fonds des utilisateurs. « Ces développeurs utilisaient des portefeuilles matériels et étaient géographiquement répartis, ce qui réduisait la probabilité d'une attaque physique coordonnée », a déclaré l'entreprise.

« Les attaquants ont pu compromettre les appareils d'au moins ces trois contributeurs principaux par le biais d'une injection sophistiquée de logiciels malveillants. Ces appareils compromis ont ensuite été utilisés pour signer des transactions malveillantes ».

Le rapport indique qu'il est probable que d'autres appareils aient été ciblés en plus des trois qui ont été compromis.

L'incident a été initialement découvert sur les médias sociaux par des chercheurs qui ont vu le pirate convertir les fonds volés en environ 12 800 ETH, d'une valeur d'environ 33,5 millions de dollars, et 32 100 BNB, d'une valeur d'environ 19,3 millions de dollars. D'autres affirment que les pertes pourraient atteindre 58 millions de dollars.

Le site web de Radiant Capital montre qu'il a fait l'objet de plusieurs audits de sécurité par d'importantes sociétés de sécurité de la blockchain, notamment Peckshield et Zokyo.

L'incident de mercredi est toutefois le deuxième piratage affectant la plateforme cette année, après le vol de 4,5 millions de dollars en janvier.

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

Comprendre le piratage d'EigenLayer : Une plongée en profondeur dans le vol de 5,7 millions de dollars

Le protocole de restaking Ethereum EigenLayer a récemment été victime d'une faille de sécurité, qui a entraîné le vol d'environ 5,7 millions de dollars en jetons. Le 4 octobre, l'équipe d'EigenLayer a révélé qu'elle enquêtait sur des activités de vente suspectes liées à une adresse de portefeuille spécifique se terminant par « f10D ». Il s'est avéré que ce portefeuille avait vendu environ 1,6 million de jetons EIGEN, ce qui a suscité l'inquiétude de la communauté cryptographique.

À la suite de son enquête initiale, EigenLayer a indiqué le 5 octobre que la vente non autorisée était effectivement le résultat d'une cyberattaque. Les attaquants avaient compromis un fil de courriels lié au transfert de jetons d'un investisseur, ce qui leur avait permis de détourner les jetons vers leur portefeuille.

En réponse au piratage d'EigenLayer, l'équipe a pris des mesures immédiates pour limiter les dégâts. Elle a contacté les plateformes et les organismes d'application de la loi concernés pour coordonner les efforts de récupération. Selon leur mise à jour, certains des fonds volés ont déjà été gelés, ce qui illustre leur approche proactive de la situation.

Le moment choisi pour la cyberattaque d'EigenLayer a suscité des inquiétudes quant à la performance globale du marché des jetons EIGEN. Le 1er octobre, après le déblocage des jetons EIGEN, le prix était fixé à 3,85 dollars sur Binance, ce qui correspondait à une évaluation entièrement diluée (FDV) d'environ 6,5 milliards de dollars, assurant une place dans le classement des 100 premiers marchés. Cependant, le 5 octobre, à la suite de la cyberattaque contre EigenLayer, la valeur du jeton est tombée à environ 3,38 dollars, ce qui correspond à une valeur pleinement diluée de 5,6 milliards de dollars et à un déclin ultérieur jusqu'à la 99e place de la capitalisation boursière.

La communauté d'EigenLayer a exprimé des réactions mitigées à l'incident, beaucoup soulignant la nécessité de renforcer les mesures de sécurité dans le paysage en évolution rapide des crypto-monnaies.

L'équipe d'EigenLayer continue d'enquêter sur l'incident et s'est engagée à tenir ses utilisateurs informés. L'objectif est de fournir des éclaircissements et des garanties afin de rétablir la confiance au sein de la communauté à la suite de la violation de données chez EigenLayer.

Source : https://bit.ly/40vrALl

Bon à savoir

L'importance de la Protection des Données Personnelles à l'Ère Numérique

La protection des données est un enjeu crucial à l'ère numérique d'aujourd'hui. Avec l'augmentation des interactions en ligne, nos informations personnelles sont souvent à portée de clic. Lorsque nous partageons des données telles que notre nom, adresse ou informations financières, nous nous exposons à divers risques. Ces informations peuvent être utilisées par des acteurs malveillants pour des actes tels que le vol d'identité, la fraude ou le harcèlement.

L'une des raisons majeures de protéger nos données personnelles est la montée de la cybercriminalité. Les hackers sont de plus en plus sophistiqués et peuvent exploiter n'importe quelle information partagée pour accéder à nos comptes ou voler notre identité. De plus, de nombreuses entreprises ne gèrent pas toujours les données de manière responsable, ce qui peut entraîner des fuites ou des violations qui compromettent notre vie privée.

Partager nos données personnelles peut également nuire à notre réputation. Une fois que quelque chose est mis en ligne, il devient difficile de contrôler son utilisation ou la façon dont il est perçu. Cela peut entraîner des conséquences graves, comme l'attention non désirée ou même la perte d'emploi.

Il est également important de se rappeler que la vie privée est un droit humain fondamental. Chacun mérite de contrôler ses propres informations sans craindre d'être exploité. En protégeant nos données, nous ne nous protégeons pas seulement nous-mêmes, mais nous contribuons également à un environnement en ligne plus sûr pour tous.

De plus, les données personnelles peuvent être vendues à des tiers sans notre consentement, augmentant ainsi le risque de profilage ou de manipulation. Enfin, la sensibilisation à la protection des données doit être une priorité pour tous, afin de garantir un avenir numérique où la vie privée est respectée. En somme, faire preuve de prudence dans le partage de nos informations personnelles est essentiel pour assurer notre sécurité et notre bien-être dans le monde numérique.

Evènements

Evènement à venir

ISC2 Spotlight : How Changed the Future of Cybersecurity 2024

6 - 7 novembre - Online

https://bit.ly/3YSoakQ

Rejoignez l'ISC2 pour un événement virtuel gratuit au cours duquel vous pourrez découvrir comment les développements récents redessinent l'avenir de la cybersécurité. Cette session engageante sera animée par des experts de l'industrie qui discuteront des tendances émergentes, des technologies et des meilleures pratiques qui révolutionnent la façon dont nous abordons la sécurité.

Vous obtiendrez des informations précieuses sur l'évolution du paysage des menaces, l'impact des nouvelles réglementations et les stratégies novatrices de protection des informations sensibles. Que vous soyez un professionnel chevronné ou un nouveau venu dans le domaine,

Référence	ANPT-2024-BV-10
Titre	Bulletin de veille N°10
Date de version	31 octobre 2024
Contact	ssi@anpt.dz