BULLETIN DE VEILLE N°09

ANPT-2025-BV-09

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

Septembre 2025

Alertes de sécurité

Cisco

Cisco met en garde contre une vulnérabilité zero-day IOS largement exploitée

24 Septembre 2025

Dans une alerte de sécurité, Cisco a annoncé qu'une vulnérabilité zero-day dans ses logiciels IOS et IOS XE est activement exploitée dans des attaques ciblées. Le défaut, catalogué CVE-2025-20352, réside dans le sous-système SNMP (Simple Network Management Protocol) et se manifeste par un débordement de tampon (stack-based buffer overflow). Lorsqu'un appareil Cisco vulnérable a SNMP activé, un attaquant authentifié (avec peu de privilèges) peut envoyer un paquet SNMP spécialement conçu via IPv4 ou IPv6 afin de déclencher un déni de service (DoS). Si l'assaillant dispose de privilèges élevés, il peut exécuter du code arbitraire à partir du niveau root, ce qui donne un contrôle total sur l'appareil compromis.

Cisco a indiqué que les attaques observées en conditions réelles résultaient d'un accès préalable aux identifiants administrateurs locaux sur l'équipement cible — autrement dit, l'attaquant devait déjà avoir un certain niveau d'accès pour exploiter pleinement la faille. Face à cette menace, Cisco recommande fortement aux clients de mettre à jour leurs systèmes vers les versions corrigées dès que possible.

Par ailleurs, Cisco a profité de cette actualité pour publier des correctifs pour 13 autres vulnérabilités, dont deux pour lesquelles des preuves de concept existent déjà. L'une est une faille XSS (cross-site scripting) dans IOS XE (CVE-2025-20240) qui pourrait permettre à un attaquant non authentifié de voler des cookies, et l'autre est une vulnérabilité de déni de service (CVE-2025-20149) pouvant être déclenchée par un attaquant local authentifié pour forcer le redémarrage de l'appareil. En mai, Cisco avait déjà corrigé une faille critique dans IOS XE affectant les contrôleurs sans fil, qui autorisait la prise de contrôle à distance via un jeton JWT codé en dur. Dans l'ensemble, ces problèmes soulignent l'importance pour les exploitants d'infrastructures réseau de surveiller de près les correctifs de sécurité, de restreindre les services non essentiels (comme SNMP), et de pratiquer une hygiène stricte d'accès et de privilèges pour limiter l'impact des attaques ciblées.

Source : https://bit.ly/49dwaia

Apple

Apple a annoncé avoir rétroporté des correctifs pour une vulnérabilité récemment corrigée et activement exploitée.

17 Septembre 2025

En août 2025, Apple a corrigé en urgence une vulnérabilité active référencée CVE-2025-43300, en la rétroportant (backport) sur plusieurs de ses systèmes : iOS, iPadOS et macOS. Il s'agissait d'un problème de "out-of-bounds write" dans le framework ImageIO, pouvant entraîner une corruption mémoire lorsqu'un fichier image malveillant était traité. Apple a reconnu qu'elle était consciente d'un rapport indiquant que cette faille avait peut-être déjà été exploitée dans une attaque sophistiquée ciblant des personnes spécifiques.

Pour combler la faille, la firme a amélioré les vérifications des bornes (bounds checking) dans le code concerné, et a poussé des mises à jour pour de nombreuses versions de ses systèmes d'exploitation. Parmi les correctifs déployés figurent iOS/iPadOS 18.6.2, les versions de macOS Ventura 13.7.8, Sonoma 14.7.8 et Sequoia 15.6.1, ainsi que des versions antérieures comme iOS 16.7.12 et iOS 15.8.5 pour couvrir les appareils plus anciens. Apple n'a cependant pas divulgué de détails techniques sur la manière dont la vulnérabilité a été exploitée dans la nature.

Cette action montre l'importance pour Apple d'agir rapidement même après la sortie initiale d'un correctif, notamment lorsqu'une faille est activement utilisée. Apple assure une protection pour les utilisateurs qui ne peuvent pas ou ne veulent pas mettre à jour vers la version la plus récente. Le cas souligne aussi le danger des vulnérabilités dans des composants communs comme les bibliothèques de traitement d'images : même un simple fichier image peut devenir un vecteur d'attaque, si le code de validation est insuffisant.

Source : https://bit.ly/49dwaia

Actualité

Red Hat confirme le piratage d'une instance GitLab et le vol de données

Red Hat a confirmé qu'une de ses instances GitLab internes, utilisée par son équipe Consulting, a été compromise par un acteur non autorisé. Les hackers, se disant membres du groupe Crimson Collective, affirment avoir exfiltré environ 570 Go de données compressées provenant de 28 000 dépôts privés. Les informations volées incluraient du code source, des configurations, des secrets, des rapports d'engagement clients (Customer Engagement Reports – CER) et des communications internes liées aux services de conseil. Red Hat a précisé que cette instance n'est pas censée contenir de données personnelles sensibles et, jusqu'à présent, n'a trouvé aucune indication d'impact sur d'autres services, produits ou sa chaîne d'approvisionnement logicielle.

Selon Red Hat, l'accès non autorisé a été détecté, puis la société a immédiatement isolé l'instance compromise, révoqué l'accès des intrus, lancé une enquête et alerté les autorités compétentes. L'entreprise indique que l'incident semble se limiter aux activités de conseil, notamment les documents relatifs aux engagements auprès de clients, les spécifications de projet, les exemples de code et les communications internes afférentes. Elle assure qu'aucune preuve n'a été trouvée suggérant que des données sensibles ont été touchées. Red Hat s'est également dite confiante dans l'intégrité de ses autres systèmes et de sa chaîne logistique logicielle.

Le groupe Crimson Collective prétend avoir ciblé des organisations de haut profil dans ses données volées, incluant des banques, opérateurs télécoms, entreprises industrielles et entités gouvernementales, ce qui pourrait exposer des architectures réseau, des jetons d'authentification, des URI de bases de données, et d'autres éléments stratégiques. En conséquence, l'Agence de cybersécurité de Belgique a émis un avis de risque élevé, recommandant aux entités concernées de révoquer immédiatement les clés, jetons et identifiants partagés avec Red Hat, de vérifier les points d'intégration, et de renforcer la surveillance des accès et événements. Red Hat a aussi renforcé ses mesures de sécurisation interne pour prévenir de futures intrusions et assure qu'elle notifiera personnellement les clients potentiellement affectés.

Source : https://bit.ly/4axx6iA

Des cyberespions chinois ont piraté des sous-traitants du ministère américain de la Défense

Pendant la période allant de juillet 2024 à juillet 2025, un groupe de cyberespionnage chinois nommé **RedNovember** a mené des attaques soutenues contre des organisations du secteur de la défense, du gouvernement, de l'aérospatial, ainsi que des prestataires légaux et industriels. Parmi ses cibles figuraient au moins deux contractants américains de la défense, mais l'ampleur de la menace était mondiale : Amérique, Europe, Asie, et Afrique ont tous été touchés. Pour parvenir à pénétrer les réseaux visés, les attaquants ont compromis des dispositifs périphériques (edge devices) tels que des routeurs, firewalls ou VPN de marques reconnues, ainsi que des portails Outlook Web Access (OWA), ce qui leur a donné un point d'entrée initial dans les infrastructures.

Une fois à l'intérieur, RedNovember a déployé des outils d'accès, de persistance et de reconnaissance. Ils ont notamment utilisé un backdoor écrit en Go appelé Pantegana, des frameworks comme Cobalt Strike et SparkRAT, ainsi que des outils open source pour les phases d'escalade et de mouvement latéral. Leurs campagnes comprenaient des reconnaissances ciblées : par exemple, des portails OWA d'États sud-américains avant des visites diplomatiques, ou des sites web de ministères des affaires étrangères. Dans certains cas, le groupe semblait avoir un accès prolongé à des organisations intergouvernementales en Asie du Sud-Est. Malgré cela, certains processus d'attaque n'ont pas été confirmés comme compromissions réussies, ce qui suggère que l'acteur espionne fréquemment avant de se lancer dans des intrusions totales.

Les méthodes de RedNovember illustrent un modèle d'attaque moderne : ils exploitent rapidement les vulnérabilités des équipements périphériques dès leur divulgation, visent les points d'accès externes moins protégés, et mettent l'accent sur la persistance et la furtivité. Leurs cibles concernent non seulement des entités gouvernementales, mais aussi des firmes de production, des institutions de recherche, ainsi que des infrastructures critiques. Leur mode opératoire montre que les réseaux restent vulnérables aux failles récemment découvertes dans les périphériques. Il montre également que les organisations doivent renforcer l'accès à la périphérie du réseau, appliquer rapidement les mises à jour de sécurité, surveiller activement les activités suspectes et séparer leurs réseaux afin de limiter la propagation des attaques.

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

Bon à savoir

Comment télécharger des applications en toute sécurité

Télécharger des applications est devenu un geste quotidien, mais le faire sans précaution peut exposer votre téléphone à des risques importants. La première règle est de n'utiliser que les boutiques officielles, comme le Google Play Store ou l'App Store d'Apple. Ces plateformes vérifient la plupart des applications avant leur publication, ce qui réduit les risques de logiciels malveillants. Évitez de télécharger des applications à partir de sites web inconnus, de liens partagés sur les réseaux sociaux ou de fichiers APK trouvés au hasard. Ce sont souvent des sources de virus ou d'espions numériques. Avant d'installer une application, prenez toujours le temps de vérifier le nom du développeur, le nombre de téléchargements et les avis des utilisateurs. Si une application

semble douteuse, contient des fautes ou demande trop de permissions, mieux vaut s'abstenir. Quelques secondes de vérification peuvent éviter de gros problèmes plus tard.

Lorsque vous installez une application, soyez attentif aux autorisations qu'elle demande. De nombreuses applications malveillantes réclament un accès inutile à vos contacts, votre caméra ou votre position GPS. Par exemple, une simple lampe de poche ne devrait pas avoir besoin d'accéder à vos messages ou à votre micro. Posez-vous toujours la question : *« Cette autorisation est-elle vraiment nécessaire ? »* Vous pouvez gérer ces permissions dans les paramètres de votre téléphone après l'installation. Pensez aussi à mettre régulièrement à jour votre système et vos applications : ces mises à jour corrigent souvent des failles de sécurité que les pirates exploitent. Et si votre téléphone vous avertit qu'une application est suspecte ou non vérifiée, prenez l'avertissement au sérieux et ne l'installez pas.

Enfin, gardez à l'esprit que la sécurité repose sur la vigilance et les bonnes habitudes. Installez un antivirus ou une application de sécurité fiable pour analyser régulièrement votre appareil. Méfiez-vous des versions "gratuites" d'applications payantes proposées sur des sites non officiels : elles cachent souvent des publicités intrusives ou des logiciels espions. Si une application ralentit votre téléphone, consomme trop de batterie ou affiche trop de pubs, désinstallez-la sans hésiter. Pensez aussi à vous déconnecter des applications que vous n'utilisez pas souvent et à supprimer celles devenues inutiles. En combinant prudence, vérifications et bons réflexes, vous pouvez profiter pleinement de votre smartphone tout en protégeant vos données et votre vie privée.

Evènements

Evènement à venir

International Conference on Cybersecurity Studies (ICCSTUD-2025)

6 Octobre 2025 - Sétif

https://www.sans.org/

L'International Conference on Cybersecurity Studies (ICCSTUD-2025) se tiendra le 6 octobre 2025 à Sétif, en Algérie. Cette conférence vise à créer une plateforme d'échange entre chercheurs, universitaires et professionnels du domaine de la cybersécurité, afin de partager connaissances, idées et innovations autour des défis technologiques et sécuritaires actuels.

Toutes les communications acceptées seront publiées dans des volumes spéciaux indexés dans des revues reconnues (Scopus, Springer, Inderscience, UGC). L'organisation est assurée par l'ISER, qui aspire à favoriser une collaboration internationale active sur les thèmes émergents de la sécurité informatique, du cyberespace et de la protection des systèmes.

Référence	ANPT-2025-BV-09
Titre	Bulletin de veille N°09
Date de version	30 Septembre 2025
Contact	ssi@anpt.dz