"Cybersecurity is much more than a matter of IT—it's a business imperative" – Stéphane Nappo

BULLETIN DE VEILLE N°08

ANPT-2025-BV-08

Août 2025

Alertes de sécurité

Microsoft

Les serveurs Microsoft SharePoint attaqué par une vulnérabilité zero-day (CVE-2025-53770)

10 Août 2025

Une vulnérabilité de haute gravité a récemment été révélée dans les configurations hybrides de Microsoft Exchange (serveur sur site, couplé à Exchange Online), sous l'identifiant CVE-2025-53786, avec un score CVSS de 8.0. La faille exploite une faiblesse dans l'authentification des environnements hybrides : un acteur ayant obtenu un accès administratif à un serveur Exchange on-premises peut escalader ses privilèges vers l'environnement cloud associé (Exchange Online), sans laisser de traces facilement détectables dans les logs Microsoft 365. Cette attaque repose sur l'abus de certificats et de jetons OAuth/S2S entre les deux environnements, permettant de se faire passer pour n'importe quel utilisateur hybride pendant jusqu'à 24 heures. Ces jetons, une fois volés, sont imbloquables et offrent un accès impuni tant que leur durée de validité n'expire pas.

La vulnérabilité a été présentée en détail par Dirk-jan Mollema (Outsider Security) lors du Black Hat USA 2025, renforçant l'urgence de prise en compte. En réaction, Microsoft a émis une alerte et CISA a publié une directive d'urgence (ED 25-02), exigeant des agences fédérales américaines de déployer les correctifs d'avril 2025, de migrer vers l'application dédiée Exchange Hybrid, de réinitialiser les credentials du service principal partagé, et d'exécuter l'outil Health Checker pour vérifier les configurations hybrides. Microsoft a même temporairement bloqué le trafic Exchange Web Services (EWS) utilisant le principal partagé pour forcer une migration sécurisée vers la nouvelle architecture hybride.

Ce cas de vulnérabilité met en lumière le risque opérationnel systémique posé par les hybrides sans isolation claire entre cloud et on-premises. Il est essentiel que toutes les organisations concernées appliquent les correctifs sans délai car l'exposition pourrait conduire à une compromission totale du domaine, avec impact majeur sur l'identité, les données et la sécurité administrative.

Source : http://bit.ly/3HswaD0

WinRAR

Une faille WinRAR 0-day très grave exploitée pendant des semaines par deux groupes

12 Août 2025

En août 2025, une vulnérabilité critique a été découverte dans WinRAR (CVE-2025-8088). Cette faille permettait à des fichiers malveillants contenus dans une archive RAR spécialement conçue d'être extraits en dehors du dossier prévu, notamment dans les répertoires de démarrage automatique de Windows. Ainsi, les attaquants pouvaient assurer l'exécution de leurs malwares à chaque redémarrage du système. Le problème provenait d'un défaut de gestion des flux de données alternatifs (ADS), et WinRAR a publié un correctif dans la version 7.13. Toutefois, comme le logiciel n'intègre pas de mise à jour automatique, les utilisateurs doivent l'installer manuellement pour se protéger.

Deux groupes ont exploité activement cette faille avant son correctif. Le premier, RomCom (aussi appelé Storm-0978 ou Tropical Scorpius), lié à la Russie, a lancé des campagnes de spear phishing entre le 18 et le 21 juillet 2025. Les attaquants utilisaient de faux CV ou candidatures pour cibler des entreprises en Europe et au Canada, dans les secteurs financiers, industriels, logistiques et de défense. Leurs archives piégées déployaient divers malwares et backdoors, comme SnipBot, RustyClaw et Mythic Agent. Le second groupe, Paper Werewolf (ou GOFFEE), a mené des attaques contre des organisations russes, probablement après avoir acheté l'exploit sur un forum du darknet pour environ 80 000 $.

Même si les chercheurs n'ont observé aucune compromission confirmée, le risque reste majeur. Cette vulnérabilité démontre la sophistication croissante de RomCom, capable d'utiliser des zero-days pour mener des opérations ciblées de cyberespionnage. Elle illustre aussi la rapidité avec laquelle différents groupes peuvent s'approprier un exploit une fois qu'il circule. Les experts recommandent donc de mettre immédiatement à jour WinRAR vers la version 7.13, d'éviter d'ouvrir des pièces jointes inattendues, d'utiliser des sources fiables pour les téléchargements et de s'appuyer sur des protections antivirus à jour afin de limiter l'exposition à ce type d'attaque.

Source : http://bit.ly/3UZTVp3

Actualité

Des chercheurs déterminent que d'anciennes vulnérabilités constituent une menace réelle pour les données sensibles dans les cloud publics.

En août 2025, lors d'un congrès de cybersécurité aux Pays-Bas, des chercheurs ont révélé qu'il était encore possible d'exploiter des vulnérabilités processeur découvertes il y a sept ans, héritées de la famille Spectre. Ces failles, supposées atténuées, s'avèrent toujours dangereuses dans des environnements cloud, où d'anciens CPU sont encore largement utilisés et où les correctifs matériels ne sont pas universels. Les protections logicielles mises en place se montrent parfois incomplètes. Les chercheurs ont nommé cette nouvelle méthode d'attaque « L1TF Reloaded », car elle combine une variante de Spectre avec la faille L1 Terminal Fault pour créer un canal de fuite de données.

Les expérimentations ont été menées sur Google Cloud, Amazon Web Services et des hyperviseurs KVM classiques. Sur Google Cloud, les chercheurs ont réussi à extraire des données sensibles, comme la clé TLS privée d'un serveur Nginx hébergé sur une machine virtuelle cible. Sur AWS, ils n'ont obtenu que des données non critiques de l'hôte, leurs tentatives visant à voler des informations invitées ayant échoué grâce aux protections offertes par le système Nitro et son hyperviseur. Ces tests ont mis en évidence que si certaines infrastructures cloud intègrent des mécanismes solides de cloisonnement, d'autres restent vulnérables à des attaques sophistiquées exploitant des failles anciennes combinées.

Les fournisseurs concernés ont réagi rapidement. AWS a expliqué que son architecture Nitro, basée sur une séparation stricte de la mémoire, protège efficacement ses clients et qu'aucune action supplémentaire n'était nécessaire. Google a appliqué des correctifs supplémentaires à son infrastructure et a récompensé les chercheurs avec une prime de plus de 150 000 $, un record dans son programme de bug bounty cloud. Cette découverte rappelle que même des vulnérabilités anciennes peuvent redevenir exploitables lorsqu'elles sont réassemblées dans de nouvelles approches, et qu'une défense en profondeur, associant innovations architecturales et réactivité des fournisseurs, reste essentielle pour protéger les environnements cloud publics face à des menaces persistantes et évolutives.

Source : http://bit.ly/4fqBnYw

Des pirates informatiques exploitent une faille Microsoft pour s'introduire dans la Chambre des communes du Canada

En août 2025, la Chambre des communes du Canada a été victime d'une cyberattaque importante qui a mis en évidence la fragilité des systèmes institutionnels face aux vulnérabilités zero-day. Des pirates informatiques ont exploité une faille critique récemment découverte dans Microsoft SharePoint, permettant l'exécution de code à distance et l'accès non autorisé à des bases de données internes. Grâce à cette brèche, les assaillants ont pu exfiltrer diverses informations sensibles, parmi lesquelles figuraient les noms des employés, leurs rôles au sein du Parlement, les emplacements de bureaux, ainsi que des détails techniques sur les ordinateurs et appareils mobiles utilisés dans l'infrastructure parlementaire.

L'incident est survenu un vendredi, entraînant une réponse rapide des autorités canadiennes. Le Centre de la cybersécurité du Canada (CSE) a été mobilisé pour travailler de concert avec l'administration parlementaire afin d'évaluer l'ampleur de la compromission et de contenir la menace. Bien que l'identité des attaquants n'ait pas été confirmée, l'exploitation d'une faille zero-day de Microsoft SharePoint suggère un niveau élevé de sophistication, laissant penser à l'implication possible d'acteurs sponsorisés par des États ou de groupes cybercriminels spécialisés dans l'espionnage institutionnel. Cet événement s'inscrit dans un contexte où des vulnérabilités critiques sont régulièrement exploitées quelques jours seulement après leur divulgation, soulignant la rapidité d'adaptation des attaquants.

Les risques découlant de cette attaque sont multiples. Les informations dérobées pourraient servir de base à des campagnes d'ingénierie sociale ou de phishing ciblé contre le personnel parlementaire, augmentant la probabilité de futures intrusions. Elles pourraient également faciliter des mouvements latéraux dans d'autres systèmes gouvernementaux interconnectés. Pour limiter ces dangers, les experts recommandent l'application immédiate des correctifs Microsoft, le renforcement des mécanismes d'authentification et de segmentation réseau, ainsi que l'adoption d'une architecture Zero-Trust. Cet incident démontre que même les institutions les plus protégées restent vulnérables si les correctifs ne sont pas appliqués rapidement, et il met en avant la nécessité d'une collaboration étroite entre gouvernements, agences de cybersécurité et éditeurs de logiciels pour anticiper et contrer les menaces émergentes.

Source : http://bit.ly/3USJq73

Bon à savoir

Que faire après un achat frauduleux

Découvrir que vous avez acheté sur un site frauduleux peut être très frustrant, voire embarrassant, mais l'essentiel est de réagir vite. La première étape consiste à couper tout contact avec le vendeur ou la plateforme et à rassembler des preuves. Faites des captures d'écran de la page du produit, de l'email de confirmation, du reçu et de tous les messages suspects reçus. Notez la date et l'heure de l'achat, le montant payé et le moyen de paiement utilisé. Conservez ces informations, elles vous seront utiles lorsque vous contacterez votre banque ou que vous déposerez une plainte. Même si vous vous sentez mal, souvenez-vous que ces arnaques touchent beaucoup de personnes et qu'agir rapidement est ce qui compte le plus.

L'étape suivante est de sécuriser votre argent et vos comptes. Contactez immédiatement votre banque ou l'émetteur de votre carte, expliquez la situation et demandez s'il est possible de bloquer la transaction ou d'engager une procédure de remboursement

(chargeback). Si vous avez payé via une carte bancaire ou un autre service sécurisé, ouvrez un litige sans attendre. Changez le mot de passe de votre banque en ligne ainsi que celui de l'adresse email utilisée pour l'achat. Vérifiez vos relevés pour repérer toute activité inhabituelle, et si vous avez communiqué des données sensibles comme votre numéro de pièce d'identité, pensez à contacter les organismes compétents pour surveiller ou geler votre crédit. Ces mesures réduisent les risques de pertes supplémentaires ou de vol d'identité.

Enfin, prenez le temps de signaler l'arnaque et de vous protéger pour l'avenir. La plupart des pays disposent d'agences de protection des consommateurs ou de plateformes officielles où l'on peut signaler une fraude. Déposez également une plainte auprès de la police si de l'argent a été volé, et prévenez vos proches si vous aviez partagé le lien du site. Supprimez les emails ou SMS suspects, et méfiez-vous des faux services "d'aide" qui pourraient vous recontacter. À l'avenir, recherchez toujours des avis indépendants sur les vendeurs, vérifiez que le site est sécurisé, et souvenez-vous que les offres trop belles pour être vraies sont presque toujours des arnaques. Même si la situation est stressante, en réagissant vite, en gardant des preuves et en restant vigilant, vous limitez les dégâts et apprenez à acheter en ligne en toute sécurité.

Evènements

Evènement à venir

Cybersecurity Risk Management MS Information Session 2025

10th September 2025 - Online

http://bit.ly/3UmCmiP

Participez à une session en ligne enrichissante consacrée à la découverte du Master en Gestion des Risques de Cybersécurité. Cet événement, prévu le 10 septembre 2025, offrira aux futurs étudiants un aperçu complet du cursus, des professeurs et des perspectives de carrière dans le domaine de la cybersécurité.

Les participants auront l'occasion d'échanger avec les représentants du programme, de poser des questions et d'obtenir des informations précieuses sur la manière dont le programme prépare les diplômés à relever les défis en constante évolution de la cybersécurité.

Référence	ANPT-2025-BV-08
Titre	Bulletin de veille N°08
Date de version	31 août 2025
Contact	ssi@anpt.dz