



BULLETIN DE VEILLE N° 01

ANPT-2026-BV-01

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

Janvier 2026

Alertes de sécurité

VMWare

Une faille de sécurité de VMware vCenter Server corrigée en 2024, est encore attaquée

23 Janvier 2026

Un bogue critique dans VMware vCenter Server est désormais activement exploité en conditions réelles, bien que le correctif ait été publié plus d'un an auparavant. La vulnérabilité principale, connue sous le nom de CVE-2024-37079, est une faiblesse de type out-of-bounds write (dépassement de mémoire) dans l'implémentation du protocole DCERPC de vCenter, qui permet à un attaquant avec accès réseau d'envoyer des paquets spécialement conçus pour déclencher une corruption mémoire et obtenir une exécution de code à distance (RCE). Cette faille est considérée comme critique avec un score CVSS très élevé (9,8). Malgré la publication de correctifs par VMware (Broadcom) en juin 2024, des preuves récentes montrent que des acteurs malveillants exploitent encore la faille – ce qui a entraîné l'ajout de CVE-2024-37079 à la liste des vulnérabilités connues exploitées activement de la CISA (Known Exploited Vulnerabilities Catalog) en janvier 2026, soulignant l'urgence d'une mise à jour large des systèmes vulnérables.

Lorsqu'un serveur vCenter est compromis, un attaquant pourrait non seulement exécuter du code arbitraire, mais aussi prendre le contrôle ou perturber les machines virtuelles gérées, accéder à des données sensibles, modifier des configurations ou pivoter latéralement vers d'autres services internes. Ces risques sont amplifiés par le fait que vCenter Server constitue souvent le cœur de l'environnement virtualisé, orchestrant des centaines voire des milliers de machines virtuelles. Des vulnérabilités similaires avaient déjà été exploitées dans le passé par des groupes sophistiqués pour obtenir un accès étendu à des environnements VMware, ce qui rend la situation actuelle d'autant plus préoccupante pour les administrateurs systèmes et équipes de sécurité.

Source : <https://bit.ly/4smapaz>

Cisco

Cisco corrige une faille de sécurité zero-day exploitée par un groupe APT lié à la Chine

16 Janvier 2026

Cisco a publié des correctifs d'urgence pour une vulnérabilité zero-day critique dans ses produits de communications unifiées, notamment Unified Communications Manager (CM) et Webex Calling Dedicated Instance, qui était activement exploitée dans la nature avant d'être corrigée. La faille, identifiée sous CVE-2026-20045 avec un score de gravité élevé (CVSS 8.2), permet à un attaquant distant non authentifié d'exécuter des commandes arbitraires sur le système sous-jacent d'un appareil vulnérable via une série de requêtes HTTP spécialement conçues.

L'exploitation réussie de ce défaut d'entrée invalide peut offrir à l'attaquant un accès utilisateur puis une élévation de privilèges jusqu'à root, ce qui signifie qu'il pourrait modifier des configurations, exfiltrer des données ou compromettre davantage l'infrastructure si l'appareil est accessible depuis Internet. Cisco a indiqué qu'il était au courant de tentatives d'exploitation en cours, renforçant l'urgence pour les administrateurs de déployer les correctifs disponibles. Les versions affectées doivent être mises à jour vers les éditions fixes ou appliquées via les fichiers de mise à jour appropriés fournis par Cisco.

Cette vulnérabilité a été ajoutée au catalogue des vulnérabilités activement exploitées (KEV) de la Cybersecurity and Infrastructure Security Agency (CISA), qui exige des agences fédérales américaines qu'elles corrigent ce problème rapidement, soulignant l'importance critique de patcher immédiatement les systèmes affectés dans les entreprises et organisations. Il n'existe actuellement aucun contournement fiable, ce qui signifie que l'application du correctif officiel est la principale mesure d'atténuation.

À retenir pour les administrateurs : appliquer les correctifs dès que possible, restreindre l'accès à l'interface de gestion, surveiller les logs et déployer des contrôles de sécurité supplémentaires pour limiter l'impact de toute tentative d'exploitation.

Source : <https://bit.ly/3MS8iLH>

Actualité

Importante fuite de données chez une entreprise exploitant 150 stations-service aux États-Unis

Un important incident de cybersécurité a touché Gulshan Management Services, Inc., une entreprise texane qui exploite plus de 150 stations-service et dépanneurs Handi Plus et Handi Stop aux États-Unis. L'entreprise a officiellement confirmé une fuite de données à grande échelle ayant exposé les informations personnelles de plus de 377 000 personnes suite à un accès non autorisé à un de ses systèmes externes entre le 17 et le 27 septembre 2025. La compromission a été détectée le 27 septembre, mais elle est restée active plusieurs jours avant d'être identifiée, laissant potentiellement les attaquants exploiter les points d'accès sans être interrompus. La notification de l'incident aux personnes concernées n'a eu lieu que le 5 janvier 2026, soit plus de trois mois après la période d'intrusion, ce qui soulève des questions sur la rapidité de détection et de réponse aux incidents.

Les informations exposées incluent des données personnelles sensibles, telles que noms, adresses, numéros de sécurité sociale (SSN), numéros de permis de conduire, pièces d'identité gouvernementales (passeport ou carte d'identité d'État), ainsi que des détails financiers comme les numéros de compte bancaire et de cartes de crédit ou de débit. Cette étendue de données est particulièrement préoccupante, car elle peut servir à des formes complexes d'usurpation d'identité, de fraude financière ou de campagnes de phishing ciblé contre les victimes. La divulgation tardive des faits a déjà entraîné des poursuites collectives (class action) contre Gulshan Management Services, certains plaignants accusant l'entreprise de ne pas avoir suffisamment sécurisé les informations personnelles de ses clients et partenaires. Les retards dans les notifications et l'absence de clarté quant à l'offre de services de surveillance de crédit ou de protection contre le vol d'identité ajoutent à la frustration des personnes impactées.

Face à cette crise, les experts en cybersécurité recommandent des mesures immédiates de protection pour les personnes touchées, notamment la surveillance proactive de leurs comptes bancaires, la mise en place d'alertes d'activité financière, et la vigilance envers les e-mails ou appels suspects pouvant tenter d'exploiter la fuite. Du côté organisationnel, l'incident met en lumière l'importance d'une sécurité renforcée des systèmes externes, de détections plus rapides d'intrusions, et d'une communication plus transparente après une compromission de données. La coordination avec les autorités étatiques, comme le dépôt de l'avis auprès du procureur général du Maine, fait partie des obligations légales, mais il est également essentiel d'offrir des

ressources concrètes de protection aux victimes. Cet événement rappelle que même les entreprises de taille moyenne, en particulier celles manipulant une grande quantité de données clients, doivent adopter des pratiques de cybersécurité robustes pour éviter des conséquences potentiellement lourdes pour des centaines de milliers de personnes.

Source : <https://bit.ly/4pewOn>

L'université Monroe affirme que la fuite de données de 2024 a touché 320 000 personnes.

Monroe University a confirmé qu'une atteinte de données en 2024 a affecté environ 320 000 personnes, dont étudiants, anciens élèves, enseignants et membres du personnel. L'université a indiqué que l'incident est survenu après qu'un acteur non autorisé a accédé aux systèmes de l'établissement, compromettant des informations sensibles stockées dans une base de données interne. Les données exposées comprenaient des identifiants personnels tels que noms complets, dates de naissance, adresses, numéros de sécurité sociale, informations sur les visas et données d'admission. Dans certains cas, des renseignements supplémentaires comme les numéros de permis de conduire ou d'état civil ont aussi été inclus. Ce type d'information peut être utilisé pour des usurpations d'identité, fraudes financières et attaques de phishing hautement ciblées contre les victimes.

L'université a déclaré avoir détecté l'incident en 2024, mais a finalisé l'analyse de l'ampleur complète des données exposées au cours des mois suivants avant de notifier les personnes concernées en 2025. Monroe University a assuré qu'elle travaillait avec des experts en cybersécurité externes pour enquêter sur la brèche, identifier les lacunes qui ont permis l'accès non autorisé et renforcer ses systèmes de protection. L'établissement a également indiqué qu'il mettait en place des services de surveillance du crédit et de protection contre le vol d'identité pour les personnes touchées. Les responsables ont invité les individus affectés à rester vigilants face à des tentatives de fraude ou de phishing, et à surveiller leurs comptes financiers et rapports de crédit pour détecter toute activité suspecte.

Cet incident rappelle que les institutions éducatives, qui gèrent souvent des volumes importants de données personnelles sensibles, sont des cibles attrayantes pour les cybercriminels. Une réponse rapide, une communication transparente et des mesures de protection post-incident sont essentielles pour limiter les dommages causés aux victimes. Les organisations similaires doivent également revoir leurs stratégies de sécurité, effectuer des audits réguliers et appliquer des contrôles stricts d'accès aux données pour éviter de futures violations. Les victimes sont encouragées à signaler toute activité inhabituelle à leurs institutions financières et aux autorités compétentes.

Source : <https://bit.ly/4pewOnp>

Bon à savoir

Que faire si votre compte de réseau social est piraté ?

Découvrir que votre compte sur les réseaux sociaux a été piraté peut-être stressant et inquiétant. La première étape est

de garder votre calme et de ne pas paniquer. Essayez immédiatement de vous connecter avec votre mot de passe habituel. Si vous ne pouvez pas accéder à votre compte, utilisez la fonction « Mot de passe oublié » ou « Récupération de compte » de la plateforme. Vérifiez votre courrier électronique pour des messages de la part du réseau social concernant une activité suspecte. Une fois que vous avez récupéré l'accès, changez votre mot de passe immédiatement et assurez-vous qu'il est fort et unique. N'utilisez pas le même mot de passe que pour d'autres comptes. Cette étape peut empêcher le pirate de reprendre le contrôle de votre compte.

Ensuite, vérifiez attentivement l'activité et les paramètres de votre compte. Recherchez les publications, messages ou demandes d'amis inhabituelles envoyées depuis votre compte. Supprimez ou signalez tout contenu publié par le pirate. Activez la double authentification (2FA) pour ajouter une couche de sécurité supplémentaire. Supprimez l'accès à toute application tierce que vous ne reconnaissez pas ou que vous n'utilisez plus. Informez vos amis et contacts que votre compte a été piraté afin qu'ils ne cliquent pas sur des liens ou messages suspects envoyés depuis votre compte. Surveillez votre compte pendant plusieurs semaines pour détecter toute activité inhabituelle. Cela permet de s'assurer que votre compte reste sécurisé et d'éviter de nouvelles attaques.

Enfin, prenez des mesures pour protéger vos autres comptes en ligne. Changez les mots de passe de votre email, de vos comptes bancaires et de tous vos autres comptes importants, au cas où le pirate aurait essayé d'y accéder également. Méfiez-vous des emails ou messages de phishing prétendant vous aider à récupérer votre compte. Signalez le piratage au service d'assistance de la plateforme et suivez attentivement leurs instructions. Apprenez de cette expérience en utilisant des mots de passe plus forts, en activant la double authentification sur tous vos comptes et en restant vigilant face aux activités suspectes. Agir rapidement et suivre ces étapes permet de réduire les dommages, de protéger vos informations personnelles et de préserver votre présence en ligne en toute sécurité.

Evènements

Evènement à venir

International Conference on Blockchain-Enhanced Cybersecurity in Big Data Analytics (ICBCBDA)

27 Février 2026 | alger, Algeria

<https://bit.ly/4jopAMv>



L'International Conference on Blockchain-Enhanced Cybersecurity in Big Data Analytics est une conférence internationale qui s'est tenue à Alger (Algérie) le 27 février 2026, réunissant chercheurs, professionnels et experts pour explorer comment la blockchain peut renforcer la cybersécurité dans l'analyse des données massives. L'évènement visait à partager des stratégies innovantes, des études de cas et des solutions pratiques, tout en offrant une plateforme de réseautage et de collaboration entre universitaires, décideurs et acteurs de l'industrie

Référence	ANPT-2026-BV-02
Titre	Bulletin de veille N°01
Date de version	30 Janvier 2026
Contact	ssi@anpt.dz