



BULLETIN DE VEILLE N° 03

ANPT-2026-BV-03

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

Mars 2026

Alertes de sécurité

Microsoft

Microsoft publie un correctif OOB pour Windows 11 afin de corriger une faille RCE dans RRAS

14 mars 2026

Microsoft a publié une mise à jour de sécurité d'urgence dite out-of-band (OOB) pour corriger plusieurs vulnérabilités critiques dans Windows 11, affectant le service Routing and Remote Access Service (RRAS). Ces failles, identifiées notamment sous les codes CVE-2026-25172, CVE-2026-25173 et CVE-2026-26111, permettent potentiellement l'exécution de code à distance si un utilisateur interagit avec un serveur malveillant. Cette mise à jour spéciale, appelée Hotpatch KB5084597, a été publiée en dehors du cycle habituel de Patch Tuesday en raison de la gravité du problème et des risques associés.

La particularité de ce correctif réside dans son mode de déploiement : il s'agit d'un Hotpatch, ce qui signifie qu'il peut être appliqué sans redémarrage du système, réduisant ainsi les interruptions pour les environnements professionnels. Le correctif cible principalement les versions Windows 11 24H2, 25H2 et Enterprise LTSC 2024, en particulier les appareils inscrits au programme Hotpatch, souvent utilisés dans des contextes d'entreprise. Les vulnérabilités concernent l'outil RRAS utilisé pour gérer les connexions distantes, et un attaquant pourrait exploiter ces failles pour exécuter du code ou perturber le système si une connexion vers un serveur malveillant est établie.

Bien que ces vulnérabilités aient déjà été partiellement corrigées lors des mises à jour de sécurité de mars 2026, cette mise à jour supplémentaire vise à protéger rapidement les systèmes critiques, notamment ceux qui ne peuvent pas se permettre des redémarrages fréquents. Microsoft précise que les systèmes non-inscrits au programme Hotpatch ont déjà reçu les correctifs via les mises à jour classiques. Cet incident met en évidence l'importance des correctifs rapides dans les environnements d'entreprise et démontre comment une seule faille dans un composant réseau peut exposer des systèmes

entiers à des attaques sophistiquées si elle n'est pas corrigée rapidement.

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

Wordpress

Une faille dans un plugin WordPress de gestion des abonnements a été exploitée pour créer des comptes administrateur

5 Mars 2026

Des hackers exploitent activement une vulnérabilité critique dans le plugin User Registration & Membership de WordPress, utilisé sur plus de 60 000 sites web. Cette faille, identifiée comme CVE-2026-1492 avec un score de gravité de 9,8, permet à des attaquants non authentifiés de créer des comptes administrateurs simplement en manipulant les données envoyées lors de l'inscription. Le problème provient du fait que le plugin accepte un rôle utilisateur fourni par l'utilisateur sans vérification côté serveur, ce qui permet d'attribuer directement des privilèges élevés.

Une fois un compte administrateur créé, les attaquants obtiennent un contrôle total sur le site compromis. Ils peuvent installer des plugins malveillants, modifier le code PHP, altérer le contenu du site, voler des bases de données d'utilisateurs ou encore injecter des malwares destinés aux visiteurs. Des chercheurs en sécurité ont déjà observé une exploitation active de cette faille, avec plus de 200 tentatives bloquées en seulement 24 heures, ce qui montre une adoption rapide par les cybercriminels. Cette compromission complète transforme les sites vulnérables en plateformes potentielles pour des campagnes de phishing, de distribution de malware ou d'hébergement d'infrastructures malveillantes. La vulnérabilité affecte toutes les versions du plugin jusqu'à la version 5.1.2 et a été corrigée dans la version 5.1.3 et suivantes. Les administrateurs de sites sont fortement encouragés à mettre à jour immédiatement leur plugin ou à le désactiver temporairement s'ils ne peuvent pas appliquer le correctif. Cet incident souligne une fois de plus que les plugins tiers représentent un point d'entrée majeur pour les attaques sur WordPress, et qu'une gestion rigoureuse des mises à jour est essentielle pour prévenir les compromissions.

Source : <https://bit.ly/41FAcyl>

Actualité

Des cybercriminels affirment avoir piraté l'administration locale de Southold, dans l'État de New York, et volé des données.

Un groupe de ransomware appelé Rhysida a revendiqué le piratage du gouvernement local de Southold, dans l'État de New York, affirmant avoir volé des données sensibles après une attaque survenue en novembre 2025. Les autorités locales avaient initialement signalé une cyberattaque ayant perturbé de nombreux services municipaux, notamment les e-mails, la paie, la collecte des taxes et les permis administratifs. Les systèmes ont été fortement impactés, obligeant la ville à fonctionner en mode dégradé pendant plusieurs jours, avec une restauration progressive sur environ deux semaines. Cependant, les responsables n'ont pas confirmé officiellement les affirmations des attaquants concernant le vol de données.

Sur son site de fuite, le groupe Rhysida a exigé une rançon de 10 bitcoins (environ 660 000 \$ au moment des faits) et a menacé de vendre les données volées si la ville refusait de payer dans un délai de sept jours. Les autorités de Southold ont clairement indiqué qu'elles n'avaient pas l'intention de payer la rançon, tout en poursuivant leur enquête avec des partenaires de cybersécurité. À ce stade, il reste incertain quelles données ont été compromises ni comment les attaquants ont initialement pénétré le réseau. L'incident souligne la difficulté pour les organisations publiques de vérifier rapidement les revendications des groupes de ransomware, qui utilisent souvent la pression médiatique pour forcer les paiements. Le groupe Rhysida, actif depuis 2023, fonctionne selon un modèle de ransomware-as-a-service, permettant à des affiliés de lancer des attaques en échange d'une part des gains. Il a déjà ciblé plusieurs organismes gouvernementaux, démontrant une tendance croissante à attaquer les institutions publiques. En 2025, des dizaines d'attaques similaires ont touché des entités gouvernementales américaines, compromettant des centaines de milliers de dossiers personnels. Ces incidents peuvent perturber des services essentiels et exposer les

citoyens à des risques de fraude et d'usurpation d'identité. L'attaque contre Southold illustre ainsi la menace persistante des ransomwares pour les infrastructures publiques et l'importance d'investir dans des mesures de cybersécurité robustes

Source : <https://bit.ly/4sL9FvB>

Le ransomware Payload revendique le piratage de l'hôpital Royal de Bahreïn

Le groupe de cybercriminels Payload Ransomware affirme avoir piraté Royal Bahrain Hospital, un établissement médical important à Bahreïn, et avoir volé environ 110 Go de données sensibles. Selon les informations publiées, les attaquants ont ajouté l'hôpital à leur site de fuite sur le dark web et ont commencé à divulguer des preuves de la compromission, notamment des captures d'écran de fichiers internes. Cette revendication s'inscrit dans la stratégie classique des groupes de ransomware consistant à combiner chiffrement et exfiltration de données pour faire pression sur leurs victimes.

À ce stade, aucune confirmation officielle détaillée n'a été fournie par l'hôpital concernant l'étendue réelle de la compromission ni sur la nature exacte des données volées. Comme dans de nombreux incidents similaires, il est possible que les données concernent des informations médicales, administratives ou financières, ce qui pourrait avoir un impact important sur la confidentialité des patients et du personnel. Le groupe de ransomware cherche généralement à forcer le paiement d'une rançon en menaçant de publier ou vendre les données si ses exigences ne sont pas satisfaites.

Cette attaque illustre une fois de plus la vulnérabilité du secteur de la santé face aux cybermenaces, en particulier aux opérations de ransomware qui ciblent des infrastructures critiques. Les hôpitaux représentent des cibles privilégiées en raison de la sensibilité des données qu'ils détiennent et de la nécessité de maintenir leurs services opérationnels en permanence. L'incident met en évidence l'importance de renforcer les mesures de cybersécurité, la surveillance des systèmes et la préparation aux incidents afin de limiter les impacts potentiels de ce type d'attaque sophistiquée.

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

Bon à savoir

Emails frauduleux : soyez vigilants

Dans un environnement professionnel, cliquer sur des liens aléatoires dans les emails peut entraîner de graves risques de sécurité. De nombreuses cyberattaques commencent par un simple message qui semble normal ou urgent. Ces emails peuvent paraître provenir de collègues, de supérieurs ou d'entreprises de confiance. Pourtant, il s'agit souvent de messages frauduleux conçus pour tromper les employés. Ce type d'attaque est appelé phishing. Lorsqu'un employé clique sur un lien malveillant, il peut télécharger un virus sans le savoir ou être redirigé vers un faux site web. Ces sites imitent souvent des plateformes légitimes afin de voler des identifiants ou des informations sensibles. Un seul clic peut compromettre un appareil et même tout

le réseau de l'entreprise. C'est pourquoi il est essentiel de toujours faire preuve de prudence avant de cliquer. Les cybercriminels utilisent différentes techniques pour rendre leurs emails crédibles. Ils créent souvent un sentiment d'urgence, comme « votre compte sera bloqué » ou « action immédiate requise ». Certains messages contiennent des liens ou des pièces jointes présentés comme des factures, des livraisons ou des alertes de sécurité. D'autres imitent des marques connues ou des services internes de l'entreprise. Avant de cliquer, il est important de vérifier l'adresse email de l'expéditeur et de repérer les détails inhabituels. Passer la souris sur le lien permet de voir la véritable destination. Si l'adresse semble étrange, mal écrite ou inconnue, il vaut mieux ne pas cliquer. En cas de doute, contactez l'expéditeur par un autre moyen pour confirmer. Pour rester en sécurité, les employés doivent adopter de bonnes pratiques. Ne cliquez jamais sur des liens provenant d'emails suspects ou inconnus. Utilisez uniquement les outils approuvés par l'entreprise et maintenez les logiciels à jour. Signalez immédiatement tout email suspect au service informatique ou à l'équipe de sécurité. Supprimer les messages dangereux permet aussi de protéger les autres collègues. La sensibilisation et la formation sont essentielles pour éviter ces attaques. En étant attentifs et prudents, les employés contribuent à protéger les données, les systèmes et la réputation de l'entreprise. Un seul clic peut causer de gros dégâts, mais une décision prudente peut éviter une cyberattaque.

Evènements

Evènement à venir

International Conference on Cybersecurity Challenges in Blockchain and Big Data (ICCCBBD)

25 Avril 2026 | Alger, Algérie
<https://bit.ly/4sWpGi8>



Rejoignez l'International Conférence on Cybersécurité Challenges in Blockchain and Big Data (ICCCBBD) le 25 avril 2026 à Alger, un événement qui rassemble chercheurs, experts, professionnels et étudiants du monde entier pour explorer les dernières avancées en cybersécurité, blockchain et big data. Participez à des ateliers interactifs, des présentations et des discussions approfondies, et échangez des idées innovantes avec vos pairs. Découvrez les projets les plus récents, inspirez-vous des leaders du secteur et établissez des collaborations internationales enrichissantes. Cet événement est une occasion unique d'apprendre, de réseauter et de contribuer activement aux débats qui façonnent l'avenir numérique. Ne manquez pas cette opportunité de renforcer vos compétences et de vous connecter à une communauté passionnée et engagée.

Référence	ANPT-2026-BV-03
Titre	Bulletin de veille N°03
Date de version	31 Mars 2026
Contact	ssi@anpt.dz