



BULLETIN DE VEILLE N° 02

ANPT-2026-BV-02

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

Février 2026

Alertes de sécurité

Apple

Apple corrige une faille zero-day exploitée dans des attaques « extrêmement sophistiquées ».

11 Février 2026

Apple a publié des mises à jour de sécurité d'urgence afin de corriger une vulnérabilité zero-day critique qui était activement exploitée dans le cadre d'attaques que l'entreprise a qualifiées d'extrêmement sophistiquées et ciblées. La faille, rapportée par BleepingComputer, affecte le composant dyld (le chargeur dynamique) utilisé dans les systèmes d'exploitation Apple et pourrait permettre à des attaquants d'exécuter du code arbitraire sur des appareils compromis. Apple a reconnu que cette vulnérabilité pourrait avoir été exploitée lors d'attaques réelles visant des personnes spécifiques, ce qui indique une menace hautement ciblée plutôt qu'une exploitation massive.

La vulnérabilité touche un large éventail d'appareils, notamment les iPhones récents, les iPads, les Mac, l'Apple Watch, l'Apple TV et le Vision Pro. Pour corriger le problème, Apple a déployé des mises à jour dans tout son écosystème. L'entreprise recommande vivement aux utilisateurs d'installer ces mises à jour immédiatement afin de réduire les risques. La faille a été découverte par le Google Threat Analysis Group, spécialisé dans la détection des activités cybernétiques avancées

Il s'agit de la première vulnérabilité zero-day corrigée par Apple en 2026, après plusieurs autres failles critiques résolues ces derniers mois. Bien qu'Apple n'ait pas révélé les détails techniques concernant le fonctionnement exact de la chaîne d'exploitation, la mention de plusieurs vulnérabilités liées suggère que les attaquants ont pu combiner différentes faiblesses pour parvenir à une compromission complète des appareils

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

BeyondTrust

Exploitation de BeyondTrust RCE pour le contrôle de domaine

16 Février 2026

Des attaquants exploitent activement une vulnérabilité critique d'exécution de code à distance affectant les produits Remote Support (RS) et Privileged Remote Access (PRA) de BeyondTrust, identifiée sous le code CVE-2026-1731. Cette faille, de type injection de commandes système non authentifiée, permet d'envoyer des requêtes HTTP spécialement conçues afin d'exécuter des commandes arbitraires sur l'apppliance sans aucune authentification préalable. Selon Arctic Wolf, des attaques réelles ont déjà été observées, menant à une compromission complète des environnements Windows. Les intrusions commencent par l'exploitation à distance, puis évoluent vers l'escalade de privilèges jusqu'à l'obtention des rôles Domain Admin et Enterprise Admin, offrant ainsi un contrôle total sur l'Active Directory.

Dans les chaînes d'attaque analysées, les cybercriminels utilisent d'abord la vulnérabilité pour exécuter des commandes système et implanter des outils de persistance, notamment des versions renommées de solutions de gestion à distance comme SimpleHelp. Ils procèdent ensuite à une phase de reconnaissance interne à l'aide de commandes telles que net share et ipconfig /all pour cartographier le réseau. L'énumération de l'Active Directory est réalisée via des requêtes LDAP ou des outils intégrés, permettant d'identifier les comptes à privilèges élevés. Les attaquants créent ensuite de nouveaux comptes administrateurs et les ajoutent aux groupes stratégiques du domaine. Enfin, ils étendent leur contrôle latéralement à d'autres systèmes à l'aide d'outils comme PSEXEC ou Impacket, consolidant ainsi leur domination sur l'infrastructure.

Les organisations concernées doivent appliquer les correctifs sans délai, restreindre l'accès aux interfaces d'administration, renforcer la surveillance des comptes à privilèges et rechercher tout indicateur de compromission. La présence de comptes administrateurs suspects ou d'outils de contrôle à distance non autorisés doit être considérée comme un signal d'alerte critique.

Cette exploitation active illustre le risque majeur que représentent les outils d'accès distant non mis à jour, en particulier lorsqu'ils sont étroitement intégrés aux services centraux comme Active Directory.

Source : <https://bit.ly/4u49koI>

Actualité

Le fabricant japonais d'outils de test de puces Advantest a été victime d'une attaque de ransomware.

Advantest, un important fabricant japonais d'équipements de test de semi-conducteurs, a confirmé avoir été victime d'une attaque de ransomware après avoir détecté une activité inhabituelle au sein de son environnement informatique le 15 février 2026. L'entreprise, basée à Tokyo et présente dans plusieurs régions du monde, a immédiatement déclenché ses protocoles de réponse aux incidents pour contenir la menace. Les systèmes affectés ont été isolés afin d'empêcher une propagation plus large, et des experts en cybersécurité externes ont été engagés pour investiguer et contenir l'incident. À ce stade, la société indique que les premières constatations suggèrent qu'un tiers non autorisé a pu accéder à certaines parties de son réseau et déployer un logiciel de rançon, mais le vecteur initial d'accès n'a pas encore été déterminé.

L'enquête sur l'incident est toujours en cours et, jusqu'à présent, Advantest n'a pas confirmé si des données sensibles de clients ou d'employés ont été compromises ou exfiltrées. L'entreprise a toutefois précisé qu'elle tiendrait directement informées les personnes concernées si des informations personnelles étaient affectées et fournirait des conseils sur les mesures de protection à prendre. Aucun groupe de ransomware n'a encore revendiqué publiquement la responsabilité de l'attaque, ce qui est inhabituel dans de nombreux cas de rançongiciels où les acteurs cherchent souvent à faire pression pour obtenir un paiement. En attendant, Advantest concentre ses efforts sur la compréhension complète de l'incident tout en renforçant ses défenses pour éviter de nouvelles intrusions.

Cet incident s'inscrit dans un contexte plus large de menace croissante de ransomware contre les entreprises technologiques et manufacturières, notamment celles impliquées dans la chaîne d'approvisionnement des semi-conducteurs, qui sont devenus des cibles attrayantes pour les cybercriminels en raison de leur rôle stratégique dans les secteurs de l'électronique, des télécommunications, des véhicules autonomes et des technologies de pointe. Les attaques contre ces infrastructures critiques peuvent non seulement perturber les opérations internes, mais aussi poser des risques étendus pour les partenaires et les clients qui dépendent de produits testés et certifiés par des fournisseurs comme Advantest. L'incident souligne l'importance pour les entreprises de maintenir des pratiques de sécurité robustes, des processus de réponse aux incidents bien testés et une vigilance constante face aux vecteurs d'attaque sophistiqués

utilisés par les cybercriminels modernes.

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

Canada Goose enquête suite à la fuite de 600 000 dossiers clients par des pirates informatiques.

ShinyHunters, un groupe de cybercriminels connu pour publier des bases de données volées, affirme avoir fuité plus de 600 000 enregistrements de clients de Canada Goose sur son site de fuite, indiquant qu'il aurait obtenu des données sensibles liées aux clients de la marque de vêtements de luxe. Ces données feraient partie d'un fichier d'environ 1,67 Go et comprendraient les noms, adresses e-mail, numéros de téléphone, adresses de facturation et de livraison, historique de commandes, ainsi que des détails partiels de paiement tels que le type de carte et les quatre derniers chiffres — suffisamment d'informations pour faciliter des attaques d'hameçonnage ou de fraude ciblée. Les enregistrements semblent liés à des transactions passées plutôt qu'à une attaque récente directement contre les systèmes internes de l'entreprise, et ils pourraient provenir d'un processus de paiement tiers utilisé auparavant dans l'écosystème de données clients.

De son côté, Canada Goose a confirmé être au courant de la publication du dataset, mais affirme n'avoir trouvé aucune preuve d'une compromission de ses propres systèmes internes. L'entreprise indique que les données semblent provenir de transactions historiques de clients plutôt qu'une violation récente de son infrastructure informatique, et elle poursuit son enquête pour déterminer l'authenticité, l'origine précise et l'étendue du fichier publié. À ce stade, Canada Goose n'a pas confirmé si des informations de paiement non masquées ont été exposées, mais souligne que les données divulguées pourraient toujours poser des risques potentiels pour la vie privée des personnes concernées, notamment par le biais de campagnes de phishing personnalisées ou d'autres formes d'usurpation d'identité.

Cet incident s'inscrit dans un contexte plus large où les groupes de fuite de données exploitent des bases de données historiques ou compromises via des tiers, même lorsque les entreprises ciblées n'admettent pas de violation interne. La situation met en lumière l'importance cruciale d'une gestion rigoureuse des données, y compris celles stockées ou traitées par des prestataires externes, ainsi que des mesures de sécurité renforcées pour prévenir l'exposition de renseignements personnels au fil du temps. Les clients potentiellement affectés sont encouragés à rester vigilants face aux tentatives d'hameçonnage, à surveiller leurs comptes et à suivre toute communication officielle émanant de Canada Goose concernant cette fuite.

Source : <https://bit.ly/40HLEsI>

Bon à savoir

Signalement des incidents de sécurité en cas de suspicion

Lorsqu'un employé soupçonne qu'un virus a infecté son ordinateur professionnel, il est essentiel d'agir rapidement et avec prudence. La première étape consiste à arrêter immédiatement d'utiliser l'appareil afin d'éviter toute propagation éventuelle.

Il ne faut pas ouvrir d'autres fichiers, cliquer sur des liens ou connecter des périphériques externes. Si possible, l'ordinateur doit être déconnecté du réseau de l'entreprise en désactivant le Wi-Fi ou en débranchant le câble réseau. Cette action permet de limiter la propagation de la menace et de protéger les autres systèmes de l'organisation. Rester calme et réagir rapidement peut réduire considérablement les dommages.

L'incident doit être signalé sans délai au service informatique ou à l'équipe de sécurité des systèmes d'information, conformément aux procédures internes de l'entreprise. L'employé doit fournir des informations précises sur les signes observés, tels que des fenêtres pop-up inhabituelles, un ralentissement du système, des programmes inconnus ou l'ouverture d'un email suspect. Indiquer l'heure approximative à laquelle le problème a été détecté peut aider à identifier l'origine de l'incident. Si cela peut être fait en toute sécurité, des captures d'écran peuvent servir de preuve. Il est important de ne pas tenter de résoudre le problème soi-même sans autorisation.

Après le signalement, l'équipe informatique analysera l'appareil et effectuera des vérifications de sécurité pour confirmer la présence éventuelle d'un virus ou d'un autre logiciel malveillant. Elle pourra isoler le poste de travail pour mener une investigation plus approfondie et procéder à la remédiation. La documentation de l'incident est essentielle pour améliorer les mesures de prévention et renforcer la sécurité globale. Un signalement rapide permet de réduire les pertes de données, d'éviter l'interruption des services et de protéger l'ensemble du réseau de l'entreprise. Chaque employé joue un rôle clé dans la cybersécurité en respectant les procédures et en agissant de manière responsable.

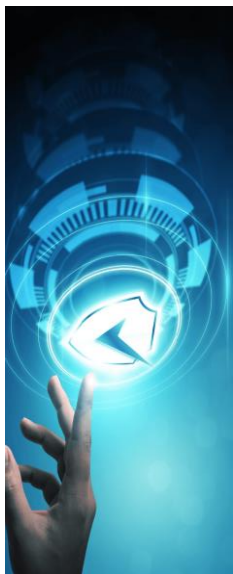
Evènements

Evènement à venir

International Conference on IT Systems Encryption and Cybersecurity Measures (ICISECM)

11 mars 2026 | Bouira, Algeria

<https://bit.ly/4r7WjYO>



La Conférence internationale sur le chiffrement des systèmes informatiques et les mesures de cybersécurité réunit des experts scientifiques en leur offrant une plateforme mondiale d'échanges académiques à travers divers événements et conférences. Elle organise des ateliers et des conférences plénières dans différents domaines, en collaboration avec des organismes locaux et des universités du monde entier. L'ISER encourage les professionnels et les chercheurs à rejoindre sa communauté afin d'utiliser la science de manière plus responsable.

Référence	ANPT-2026-BV-02
Titre	Bulletin de veille N°02
Date de version	28 Février 2026
Contact	ssi@anpt.dz