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

BULLETIN DE VEILLE N°11

ANPT-2025-BV-11

Novembre 2025

Alertes de sécurité

Firefox

Une faille critique dans Firefox expose 180 millions d'utilisateurs.

24 Novembre 2025

Une faille très critique — référencée CVE-2025-13016 — a été découverte dans le moteur WebAssembly de Firefox. Cette vulnérabilité, issue d'une erreur subtile dans la gestion de la mémoire (mauvais calcul de pointeurs dans la logique de collecte des déchets mémoire), provoque un dépassement de tampon sur la pile (stack buffer overflow), ce qui peut altérer des zones mémoire sensibles. Ce bug est présent depuis avril 2025 dans les versions 143 à 145 de Firefox, ainsi que dans les versions ESR antérieures à 140.5. Pendant près de six mois, avant la publication du correctif le 11 novembre 2025, plus de 180 millions d'utilisateurs actifs du navigateur ont été potentiellement exposés à un risque d'exécution de code arbitraire — simplement en visitant une page Web malveillante exploitant WebAssembly.

L'exploitation de cette vulnérabilité nécessite un contexte précis (pression mémoire élevée, déclenchement de la collecte des déchets, etc.), ce qui rend l'attaque non triviale. Toutefois, la gravité reste élevée : un attaquant pourrait profiter de ce bug pour exécuter du code malveillant sur la machine de l'utilisateur, compromettre des sessions, voler des données sensibles ou installer des logiciels indésirables. La très large portée de Firefox — présent sur Windows, Linux, macOS et Android — augmente l'impact potentiel de cette faille de sécurité.

Face à cette situation, il est impératif que tous les utilisateurs de Firefox mettent à jour immédiatement leur navigateur vers la version 145 ou supérieure (ou ESR 140.5+). En parallèle, les administrateurs système et les équipes de sécurité doivent bloquer ou restreindre l'utilisation de contenus WebAssembly non vérifiés, renforcer la surveillance des processus navigateur, et éventuellement appliquer des politiques d'isolation ou de sandbox renforcées pour les environnements sensibles. Cette alerte souligne l'importance cruciale de la sécurité mémoire et de la réactivité dan0s le cycle des correctifs pour les navigateurs d'usage courant, surtout dans un contexte où WebAssembly devient omniprésent.

Source : https://bit.ly/3KxOMDa

Microsoft

Microsoft a annoncé 63 correctifs affectant 13 familles de produits.

12 Novembre 2025

En novembre 2025, Microsoft a publié une mise à jour de sécurité corrigeant un total d'environ 63 vulnérabilités réparties sur 13 familles de produits (Windows, Office, Azure, SQL, etc.). Parmi celles-ci, quatre sont classées « Critiques » par l'éditeur, tandis que neuf présentent un score CVSS de 8.0 ou plus.

Un point particulièrement alarmant : une vulnérabilité zero-day, c'est-à-dire déjà largement exploitée, a été colmatée — un signal fort pour inciter à appliquer sans délai les correctifs.

Les types de menaces corrigées ce mois-ci couvrent un spectre large : élévation de privilèges, exécution de code à distance, divulgation d'information, contournement de sécurité, et déni de service. Les failles affectaient des composants critiques comme le noyau Windows, les services réseau (drivers WinSock, Hyper-V), les services cloud, ainsi que des produits à large diffusion comme Office ou les services liés à Azure.

Pour certains systèmes — notamment des serveurs ou postes sensibles — ces corrections sont d'autant plus urgentes que les vulnérabilités pouvaient permettre une compromission complète.

Face à ces risques, il est fortement recommandé d'adopter une stratégie de mise à jour immédiate. Priorisez l'installation des patchs pour Windows, puis pour Office, Azure et autres services exposés. Contrôlez les journaux système après mise à jour, vérifiez l'intégrité des sauvegardes avant déploiement, et assurez-vous que les systèmes critiques (serveurs, postes sensibles) sont protégés. Enfin, renforcez la surveillance et la défense contre l'exécution de code ou l'élévation de privilèges — un patch ne suffit pas parfois, un durcissement supplémentaire et des contrôles actifs restent nécessaires.

Source : https://bit.ly/48q6Cjv

Actualité

Une fuite de données chez un important fournisseur de logiciels suédois touche 1,5 million de personnes

Miljödata — prestataire de systèmes informatiques pour environ 80 % des municipalités suédoises — a été victime d'une cyberattaque grave. Lors de l'incident, les attaquants ont exigé une rançon de 1,5 Bitcoin pour ne pas divulguer les données volées. Malgré cette tentative d'extorsion, les informations auraient été publiées sur le dark-web, entraînant la fuite de données personnelles massives concernant jusqu'à 1,5 million de personnes. Parmi les victimes, des citoyens de nombreuses municipalités réparties sur tout le territoire suédois (halland, Gotland, Skellefteå, Kalmar, Karlstad, Mönsterås, …) — autant d'individus potentiellement exposés à des risques d'usurpation d'identité et de fraude.

Les données divulguées sont particulièrement sensibles : noms, adresses physiques, adresses mail, numéros de téléphone, numéros d'identification gouvernementaux, dates de naissance, et dans certains cas des informations liées à l'emploi ou à des services administratifs (certificats médicaux, dossiers RH, etc.). Cette situation met en lumière les dangers liés à la concentration des fonctions administratives — une seule entité compromise suffit à exposer des millions de dossiers personnels. Face à l'ampleur de l'attaque, la Swedish Authority for Privacy Protection (IMY) a ouvert une enquête pour évaluer d'éventuelles violations du règlement de protection des données (GDPR), notamment en ce qui concerne le traitement des données sensibles des enfants, des personnes sous protection spéciale ou des anciens employés des municipalités concernées.

Les conséquences sont lourdes pour les citoyens concernés comme pour les institutions publiques : perte de confiance, obligations légales de notification, risque élevé d'usurpation d'identité, fraude financière, et coûts potentiels liés aux compensations et à la remédiation. Pour limiter les risques futurs, il est essentiel de revoir profondément la sécurité des prestataires tiers — segmentation des accès, chiffrement des données sensibles, authentification forte, audits réguliers, sauvegardes hors ligne et plan de réponse aux incidents. Ce cas illustre de façon cruelle combien la résilience numérique des services publics repose autant sur des bonnes pratiques de sécurité que sur la robustesse technique des systèmes — la compromission d'un maillon faible peut produire un effet domino à l'échelle nationale.

Source : https://bit.ly/4rsN3zx

Une société canadienne de conseil scientifique confirme une violation de données suite à une demande de rançon de 1,2 million de dollars

JASCO Applied Sciences — une société canadienne de conseil scientifique — a découvert un accès non autorisé à ses systèmes informatiques. Cette intrusion a été revendiquée en octobre 2025 par le groupe de ransomware Rhysida, qui a exigé une rançon d'environ 1,22 million de dollars américains pour la suppression des données volées. Initialement, l'entreprise pensait que seules des données professionnelles non sensibles étaient concernées. Cependant, le 20 octobre 2025, JASCO a dû reconnaître que des informations personnelles sensibles (identités, numéros de sécurité sociale, coordonnées bancaires, numéros de permis de conduire, passeports, etc.) avaient aussi été compromises.

À ce jour, 66 résidents des États-Unis ont été officiellement notifiés de la fuite de leurs données, mais le nombre total de personnes affectées — incluant des employés canadiens et d'autres nationalités — pourrait être beaucoup plus élevé. Les documents fournis par Rhysida incluent des captures d'écran de cartes d'identité, ce qui confirme l'authenticité de l'exfiltration. En tant qu'acteur tiers intervenant dans de nombreux secteurs — énergie, environnement, défense, construction marine, etc. — JASCO représente ce qu'on appelle un "maillon critique" : compromettre ce type de fournisseur peut exposer indirectement les clients et partenaires à des risques de fuite ou d'extorsion, étendant l'impact de la brèche bien au-delà de la société initiale.

Cet incident démontre une fois de plus l'importance de renforcer la sécurité des prestataires externes, surtout ceux qui manipulent des données sensibles et servent de pont entre plusieurs industries. Il est désormais impératif pour JASCO et les entreprises similaires de procéder à un audit forensique complet, de révoquer les accès compromis, d'alerter toutes les personnes potentiellement affectées, et d'envisager des protections renforcées : authentification multifacteur, chiffrement des données sensibles, sauvegardes régulièrement testées, et segmentation stricte des environnements sensibles. Enfin, ce type d'attaque illustre combien la chaîne logistique numérique est vulnérable : chaque fournisseur externe représente un point d'entrée potentiel, et la sécurité globale dépend de la résilience de l'ensemble de ces maillons.

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

Bon à savoir

Que faire si votre téléphone est volé

Se faire voler son téléphone peut être stressant et effrayant, mais le plus important est de rester calme et de privilégier votre sécurité. Ne poursuivez pas le voleur et n'essayez pas de le confronter : votre sécurité physique est plus importante que n'importe quel appareil. Utilisez un autre téléphone ou un ordinateur le plus rapidement possible pour vous connecter à votre compte et activer la fonction « Localiser mon appareil » sur Android ou « Localiser mon iPhone » sur Apple. Consultez la carte pour voir si le téléphone est localisable en toute sécurité. S'il est à proximité et que vous vous trouvez dans un endroit sûr, vous pouvez tenter de le récupérer en suivant les instructions officielles. Si la récupération est impossible, verrouillez l'appareil à distance pour empêcher tout accès à vos données personnelles. Configurez un message sur l'écran de verrouillage avec une option de contact d'urgence si disponible. Vous pouvez également faire sonner le téléphone à distance pour aider à le localiser, mais seulement si vous pouvez le faire en toute sécurité. Dans les cas les plus graves, effectuez un effacement à distance pour supprimer toutes les données personnelles de l'appareil avant

qu'il ne soit utilisé à mauvais escient. Ensuite, contactez immédiatement votre opérateur mobile pour bloquer votre carte SIM et suspendre les appels, les SMS et les frais de données. Demandez-lui de vous fournir une carte SIM de remplacement pour votre nouveau téléphone. Changez vos mots de passe en commençant par votre messagerie, votre identifiant Apple ou votre compte Google, puis mettez à jour ceux de vos applications bancaires, de vos réseaux sociaux et de votre espace de stockage cloud. Activez l'authentification à deux facteurs partout où c'est possible afin de renforcer la sécurité de vos comptes. Vérifiez attentivement vos relevés bancaires et l'activité de vos applications pour détecter toute transaction ou connexion suspecte. Signalez immédiatement toute activité inhabituelle à votre banque et mettez en sécurité toutes les cartes de paiement associées à votre téléphone. Déclarez le vol à la police et fournissez le numéro IMEI si vous le connaissez. Demandez une copie du rapport de police pour vos démarches auprès de votre assurance et pour constituer un dossier officiel ; cela peut également empêcher la revente de l'appareil volé.

Si votre téléphone était utilisé à des fins professionnelles, prévenez votre employeur ou le service informatique afin que les données de l'entreprise puissent être sécurisées ou effacées à distance. Avertissez votre famille, vos amis et vos collègues du vol de votre téléphone, car des voleurs pourraient tenter d'usurper votre identité et vous envoyer des messages frauduleux. Ne répondez à aucune demande suspecte provenant de votre ancien numéro ou des comptes associés. Une fois la situation maîtrisée, remplacez votre appareil et restaurez vos fichiers à partir de sauvegardes cloud, si vous en avez. Renforcez la sécurité de votre nouveau téléphone avec un code PIN plus long, un verrouillage biométrique, des outils de géolocalisation et des sauvegardes automatiques. Évitez de laisser votre téléphone sans surveillance dans les lieux publics et soyez prudent dans les endroits fréquentés. Bien que la perte d'un téléphone soit contrariante, agir rapidement et suivre les bonnes pratiques de sécurité réduit considérablement le risque d'usurpation d'identité et de pertes financière

Evènements

Evènement à venir

International Conference on Computer Science, Programming and Security (Iccsps)

10th Décember 2025 - Setif

https://bit.ly/3MqedcS

Cette conférence internationale, répertoriée sur la plateforme International Conference Alerts, réunit des chercheurs, professionnels et experts de différents domaines pour partager leurs travaux, échanger des idées et discuter des enjeux actuels liés à l'innovation, à la recherche et au développement. L'événement vise à favoriser le réseautage, les collaborations académiques et professionnelles, ainsi que la diffusion de connaissances à l'échelle internationale, dans un cadre propice aux échanges et au renforcement des compétences.

Référence	ANPT-2025-BV-011
Titre	Bulletin de veille N°011
Date	30 Novembre 2025
Contact	ssi@anpt.dz