« In a connected world, cybersecurity is a shared responsibility.»

BULLETIN DE VEILLE N°06

ANPT-2025-BV-06

Juin 2025

Alertes de sécurité

Outlook

Vulnérabilité d'Outlook permettant l'exécution de code arbitraire à distance par des attaquants

11 juin 2025

Microsoft a récemment confirmé l'existence d'une faille de sécurité critique dans Outlook, identifiée sous le nom CVE-2025-47176. Cette vulnérabilité permettrait à un attaquant distant d'exécuter du code arbitraire sur l'ordinateur de la victime, simplement en envoyant un courriel spécialement conçu. Le danger est particulièrement élevé, car l'exploitation pourrait se produire sans interaction de l'utilisateur : il suffirait qu'Outlook traite automatiquement le contenu du message pour que l'attaque soit lancée. Cela ouvre la voie à des compromissions silencieuses, rendant cette faille extrêmement préoccupante pour les entreprises comme pour les particuliers.

Le cœur du problème réside dans la manière dont Outlook gère certains chemins de fichiers et objets intégrés. Un attaquant peut manipuler ces éléments dans un e-mail de façon à tromper Outlook et provoquer l'exécution de code malveillant. Selon les premières analyses, cette vulnérabilité impliquerait une forme de traversée de répertoire combinée à des noms de fichiers mal formés. Il s'agirait d'une attaque dite "zero-click", c'est-à-dire qui ne nécessite aucun clic de l'utilisateur. Cela rend la détection et la prévention de l'attaque d'autant plus complexes, en particulier si aucun logiciel de sécurité avancé n'est déployé.

Les experts recommandent de mettre en place des mesures temporaires de mitigation. Il est conseillé de désactiver l'aperçu automatique des e-mails dans Outlook, de limiter les privilèges des utilisateurs, et de surveiller les journaux systèmes pour repérer des comportements anormaux. Les entreprises doivent également configurer leurs solutions de filtrage pour bloquer les pièces jointes suspectes. Microsoft a annoncé qu'un correctif serait diffusé prochainement via Windows Update et les canaux Microsoft 365. En attendant, la vigilance est de mise pour éviter toute compromission via cette faille critique.

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

Wordpress

Analyse d'un plugin WordPress malveillant : The Covert Redirector

15 Mai 2025

Sucuri (entreprise spécialisée dans la sécurité web) a récemment enquêté sur un plugin WordPress malveillant nommé "wordpress-player.php", détecté sur au moins 26 sites infectés, notamment via des installations piratées ou compromises. L'extension se faisait passer pour un composant légitime de WordPress, ce qui permettait aux administrateurs de ne pas détecter immédiatement sa présence. Une fois installé dans wp-content/plugins/, il injectait du code JavaScript et HTML dans le pied de page (wp_footer), déclenchant des redirections indésirables chez les visiteurs, environ 4 à 5 secondes après leur arrivée sur le site

Techniquement, la menace repose sur un lecteur vidéo HTML5 invisible et une connexion WebSocket malveillante. Le plugin insérait un lecteur vidéo silencieux pointant vers un domaine louche, probablement pour générer de fausses impressions publicitaires, tout en restant invisible pour les visiteurs. En parallèle, le script JavaScript établissait une connexion WebSocket persistante vers un serveur C2, permettant aux attaquants d'envoyer des commandes en temps réel – telles que redirection, pause ou reprise de la vidéo – et d'identifier chaque visiteur avec un identifiant pseudo-aléatoire. L'attaque était évasive envers les utilisateurs connectés (administrateurs ou éditeurs), activant son code uniquement pour les visiteurs non connectés.

Les conséquences pour les sites infectés sont graves, avec des risques SEO, réputationnels et sécuritaires considérables. Les visiteurs sont redirigés vers des sites tiers potentiellement dangereux (phishing, malvertising, kits d'exploitation), ce qui mine la confiance des utilisateurs et peut provoquer un classement défavorable dans les moteurs de recherche. Pour contenir la menace, Sucuri recommande : scanner l'intégralité du site, supprimer wordpress-player.php et tout code malveillant, réinitialiser les identifiants administratifs, activer l'authentification à double facteur, mettre à jour WordPress et plugins, et déployer un pare-feu applicatif (WAF)

Source: https://bit.ly/4nAZG9T

Actualité

Une attaque par ransomware a contribué au décès d'un patient, déclare le NHS britannique

En juin 2024, un groupe de cybercriminels a ciblé Synnovis, un prestataire de services de pathologie basé à Londres, par le biais d'une attaque par ransomware. Synnovis fournissait des analyses sanguines vitales à plusieurs hôpitaux du NHS, dont le prestigieux King's College Hospital et Guy's and St Thomas'. L'attaque a gravement perturbé la capacité à mener à bien des tests sanguins essentiels, retardant les résultats pour des milliers de patients en attente d'un diagnostic ou d'un traitement urgent. Les retards ont forcé les hôpitaux à annuler plus de 10000 rendez-vous, y compris des procédures critiques ou des transfusions de sang, plongeant l'ensemble du système dans une vraie crise de continuité des soins.

Le ransomware employé par le groupe, identifié comme appartenant au collectif Qilin, réclamait une rançon estimée à 50 millions de dollars, un montant jamais versé. En réaction, les opérateurs ont exfiltré quelque 400 Go de données médicales sensibles, qui se sont ensuite retrouvées sur le dark web, exposant des informations confidentielles de patients. Plus gravement, l'impact sur les délais de diagnostic s'est avéré fatal pour un patient, décédé le 3 juin 2024 au King's College Hospital. L'enquête interne a conclu que le retard critiques dans les résultats sanguins avait directement contribué à l'échec des soins et figurait parmi les causes contributives de la mort.

Outre ce cas tragique, l'attaque a eu des répercussions larges et graves sur l'ensemble du système de santé. Les hôpitaux ont été contraints de gérer une pénurie de sang O-, mettant en péril des opérations chirurgicales ou des traitements urgents. Au total, environ 170 incidents liés à des préjudices aux patients ont été recensés, certains avec conséquences sérieuses, incluant des diagnostics différés ou des traitements compromis. Les effets sur la confiance publique et la réputation des établissements impactés ont été profonds, et les perturbations ont duré des semaines, laissant des séquelles dans la gestion hospitalière.

Ce drame met en évidence que les cyberattaques ne sont plus de simples problèmes informatiques : elles représentent un risque existentiel pour la sécurité des patients. Les conséquences peuvent être mortelles lorsqu'elles affectent des infrastructures médicales critiques. L'incident souligne la nécessité pour le NHS et ses prestataires tiers de rehausser leur niveau de cybersécurité, d'implémenter des plans de continuité robustes, et de considérer la sécurité numérique comme une question de vie ou de mort.

Il est devenu urgent d'établir une enquête indépendante sur la cybersécurité du NHS, afin d'évaluer les failles systémiques et de proposer des solutions durables. Les structures hospitalières doivent renforcer leurs défenses, notamment via des sauvegardes régulières, des mécanismes de restauration rapides, et des tests de résilience face aux ransomware. Ce cas constitue un signal d'alarme : face à une menace croissante, les établissements de santé doivent intégrer la cybersécurité au cœur de leurs priorités, car l'absence de protection adéquate met en jeu la vie des patients.

Source : ***https://bit.ly/4lwt2ok***

Une attaque DDoS massive de 7,3 Tbps délivre 37,4 TB en 45 secondes, ciblant un fournisseur d'hébergement

Une attaque DDoS sans précédent a été enregistrée récemment, visant un prestataire d'hébergement, avec un pic de bande passante de 7,3 térabits par seconde. En à peine 45 secondes, l'attaque a généré 37,4 téraoctets de trafic malveillant vers une seule adresse IP. Cette puissance équivaut à des milliers d'heures de vidéo HD transférées en moins d'une minute. L'attaque a été qualifiée de multivecteur, principalement fondée sur des floods UDP et des techniques d'amplification utilisant des protocoles comme NTP, Echo ou QOTD. Chaque seconde, des dizaines de milliers de ports étaient ciblés, saturant complètement les ressources de la victime.

Derrière cette offensive se cachaient plus de 122 000 adresses IP uniques, réparties dans 161 pays et provenant de plus de 5 000 réseaux autonomes (AS). Le flux malveillant atteignait des pics de 45 000 IPs actives par seconde, prouvant qu'un très grand botnet était mobilisé. Ce type d'attaque exploite souvent des objets connectés mal sécurisés, tels que des caméras, routeurs ou enregistreurs numériques, transformés à distance en "armes numériques". La nature brève mais extrêmement intense de l'attaque démontre une évolution dans la stratégie : frapper vite et fort, avant que les défenses ne puissent réagir.

Heureusement, l'infrastructure de protection de Cloudflare, via Magic Transit, a pu absorber l'attaque sans interruption de service. Ce système répartit automatiquement le trafic sur un réseau mondial de centres de données, neutralisant les surcharges en temps réel. Ce cas met en évidence l'importance croissante des défenses automatisées et distribuées face aux menaces DDoS modernes. Il rappelle aussi que même les fournisseurs les mieux protégés ne sont pas à l'abri de telles offensives, et que la cybersécurité préventive, la détection rapide et la résilience réseau sont devenues indispensables pour toute organisation connectée.

Source : https://bit.ly/4nBMOk5

Bon à savoir

Comment sécuriser votre smartphone

Votre smartphone contient vos photos, vos messages, vos contacts, vos comptes bancaires et plus encore. Il faut donc le protéger sérieusement, et pour le protégé, vous devez suivre les points suivants :

- Commencez par activer un code PIN solide, ou mieux, utilisez votre empreinte ou la reconnaissance faciale.

- Évitez les codes faciles comme 0000 ou votre date de naissance.
- Assurez-vous que le téléphone se verrouille automatiquement après quelques secondes sans activité. Installez toujours les mises à jour proposées : elles corrigent des failles que les pirates peuvent exploiter. Beaucoup de gens les ignorent, mais elles sont essentielles.
- Ne téléchargez des applications que depuis Google Play ou l'App Store. Ne faites jamais confiance à des liens envoyés par message ou trouvés sur internet. Avant d'installer une appli, vérifiez les avis et les permissions qu'elle demande. Une application météo n'a pas besoin d'accéder à votre micro, par exemple.
- Pensez à activer la double authentification (2FA) pour vos comptes importants : email, réseaux sociaux, banque. Cela ajoute une protection même si quelqu'un connaît votre mot de passe. N'utilisez jamais le même mot de passe partout, et pensez à un gestionnaire de mots de passe pour vous aider.
- Évitez les Wi-Fi publics non sécurisés. Si vous devez en utiliser, passez par une application VPN. Ne cliquez pas sur les liens suspects reçus par SMS ou WhatsApp, surtout ceux qui parlent de colis, d'amendes ou de comptes bloqués. C'est souvent du phishing.
- Activez la fonction "Localiser mon appareil" (Android ou iPhone) : elle permet de le retrouver, de le faire sonner ou même d'effacer ses données à distance en cas de vol. Enfin, sauvegardez régulièrement vos données, pour ne rien perdre si le téléphone est perdu.

Ces gestes simples vous protègent des vols de données, des arnaques et des mauvaises surprises. Prenez le temps de les appliquer.

Evènements

Evènement à venir

World Wide CTF 2025

26 - 28 Juillet 2025 - Online

https://bit.ly/4lhZFGj

Plongez au cœur de World Wide CTF 2025, un défi en ligne de type Jeopardy se déroulant du 26 au 28 juillet 2025, à partir de 12 h UTC. Cet événement international rassemblera une communauté mondiale de passionnés et d'experts en cybersécurité, prêts à tester leurs compétences dans des catégories variées : exploitation web, forensique, reverse engineering, crypto, et bien plus encore
Organisé par World Wide Flags, ce CTF est conçu pour défier tous les niveaux, qu'il s'agisse de débutants curieux ou de redoutables compétiteurs. L'objectif ? Résoudre un maximum d'épreuves, accumuler des points et, pourquoi pas, viser l'un des meilleurs classements mondiaux .

Référence	ANPT-2025-BV-06
Titre	Bulletin de veille N°06
Date de version	30 juin 2025
Contact	ssi@anpt.dz