
# BULLETIN DE VEILLE N°3

ANPT-2021-BV-03

« La culture de sécurité peut accomplir plus que la posture d'interdiction.»
- Stéphane Nappo-

Mars 2021

# Alertes de sécurit

## Microsoft

### Microsoft publie des correctifs de sécurité pour 89 failles

09 mars 2021

Microsoft a corrigé jusqu'à 89 failles de sécurité dans le cadre de ses mises à jour mensuelles du Patch Tuesday, y compris des correctifs pour un zero-day activement exploité dans Internet Explorer qui pourrait permettre à un attaquant d'exécuter du code arbitraire sur les machines cibles.

Pour le zero-day d'Internet Explorer référencé CVE-2021-26411, la société sud-coréenne de cybersécurité ENKI, qui a révélé publiquement la faille au début du mois dernier, a affirmé que les pirates de l'État-nation nord-coréen avaient tenté en vain de cibler ses chercheurs en sécurité avec des fichiers MHTML malveillants qui, une fois ouverts, téléchargeaient deux charges utiles à partir d'un serveur distant, dont un contenait un zero-day contre Internet Explorer […].

IL est fortement recommandé d'installer les dernières mises à jour de sécurité en allant vers Démarrer> Paramètres> Mise à jour et sécurité> Windows Update, ou en sélectionnant Rechercher les mises à jour Windows.

***Source*** *: https://bit.ly/2QXT6zH*

## Google

### Deux bugs de Google Chrome 0-Day trouvés activement exploités dans la nature

12 mars 2021

Chrome 89.0.4389.90, publié par Google pour Windows, Mac et Linux, contient un total de 47 correctifs de sécurité, dont le plus grave concerne un «problème de cycle de vie des objets dans l'audio».

Google a reconnu qu'un exploit pour les vulnérabilités CVE-2021-21166 et CVE-2021-21193 existe dans la nature mais s'est arrêté avant de partager plus de détails pour permettre à une majorité d'utilisateurs d'installer les correctifs et d'empêcher d'autres acteurs de la menace de créer des exploits ciblant ce zero-day.

Les utilisateurs de Chrome doivent mettre à jour vers la dernière version via : Paramètres> Aide> À propos de Google Chrome pour atténuer le risque associé à la faille.

***Source***: *http://bit.ly/3cV6cVs*

## Wordpress

### La vulnérabilité WP Super Cache affecte plus de 2 millions de sites

16 mars 2021

Une vulnérabilité a été découverte dans WP Super Cache Automattic. La vulnérabilité pourrait permettre à un pirate de télécharger et d'exécuter du code malveillant, généralement dans le but de prendre le contrôle du site.

Toutes les versions Plugin WordPress WP Super Cache <= 1.7.1 sont vulnérables. Aucun détail n'a été publié sur le type d'authentification nécessaire pour l'exploit.

Automattic, le développeur de WP Super Cache a mis à jour le logiciel. Les éditeurs qui utilisent le plugin sont invités à envisager de passer à la dernière version 1.7.2.

***Source*** *: http://bit.ly/30OZRVR*

### La vulnérabilité de WordPress Elementor affecte +7 millions sites

20 mars 2021

Les chercheurs en sécurité de Wordfence ont découvert une vulnérabilité sur des sites construits avec Elementor. La faille est désignée comme une vulnérabilité XSS (Stored Cross-site Scripting). Elle a le potentiel de permettre aux attaquants de prendre le contrôle d'un site Web. Un script malveillant peut faire un certain nombre de choses comme voler des cookies, des identifiants de mot de passe, etc.

Wordfence recommande à tous les utilisateurs d'Elementor de mettre à jour leur version à au moins 3.1.4. Il serait recommandé de mettre à jour vers la toute dernière version disponible Elementor Pro 3.2.0.

***Source***: *http://bit.ly/390i7QT*

## Github

### GitHub corrige un bug qui oblige les utilisateurs à se connecter à d'autres comptes

09 mars 2021

GitHub a automatiquement déconnecté de nombreux utilisateurs en invalidant leurs sessions GitHub.com pour protéger les comptes d'utilisateurs contre une vulnérabilité de sécurité potentiellement grave.

Le comportement anormal découle d'une vulnérabilité de condition de concurrence plutôt rare, dans laquelle la session de connexion d'un utilisateur GitHub a été mal acheminée vers le navigateur Web d'un autre utilisateur connecté, donnant à ce dernier un cookie de session authentifié et un accès au compte d'un autre utilisateur. Il est important de noter que ce problème n'était pas le résultat d'une compromission de mots de passe de compte, de clés SSH ou de jetons d'accès personnels (PAT). Au lieu de cela, ce problème était dû à la gestion incorrecte rare et isolée des sessions authentifiées.

Un correctif a été publié le 8 mars pour renforcer la sécurité du site Web.

***Source*** : *http://bit.ly/3f4jiT0*

## Linux

### Trois failles dans le noyau Linux depuis 2006 pourraient offrir des privilèges root aux attaquants

22 mars 2021

Trois vulnérabilités récemment découvertes dans le noyau Linux, situées dans le module iSCSI utilisé pour accéder aux installations de stockage de données partagées, pourraient accorder des privilèges root à toute personne disposant d'un compte utilisateur. Le trio de failles référencées - CVE-2021-27363, CVE-2021-27364 et CVE-2021-27365 – étaient restées indetéctées au sein du code Linux depuis 2006, jusqu'à ce que les chercheurs du GRIMM les découvrent.

Les bugs ont été corrigés dans les versions suivantes du noyau : 5.11.4, 5.10.21, 5.4.103, 4.19.179, 4.14.224, 4.9.260 et 4.4.260. Tous les noyaux plus anciens sont en fin de vie et ne recevront pas de correctifs.

***Source***: *https://bit.ly/3dcBgAi*

## OpenSSL

### OpenSSL corrige deux vulnérabilités de gravité élevée

26 mars 2021

Le projet OpenSSL a publié cette semaine la version 1.1.1k pour corriger deux vulnérabilités de haute gravité, respectivement référencée CVE-2021-3450 et CVE-2021-3449. Dont une liée à la vérification d'une chaîne de certificats et une qui peut déclencher une condition DoS.

Les versions 1.1.1h et plus récentes d'OpenSSL sont vulnérables. Les applications qui utilisent une version vulnérable d'OpenSSL doivent être mises à niveau vers OpenSSL 1.1.1k dès que possible.

***Source :*** *https://bit.ly/2P5b7vl*

## Apple

### Le système de suivi de l'emplacement des appareils d'Apple pourrait révéler les identités des utilisateurs

09 mars 2021

Les chercheurs ont découvert deux vulnérabilités dans l'application Offline Finding (OF), qui pourraient compromettre la confidentialité des utilisateurs.

Lors de l'upload et du téléchargement de rapports de localisation, les propriétaires d'appareils dévoilent leur identité à Apple. De plus, l'entreprise peut stocker les données pour une exploitabilité potentielle. Pour que cette faille soit exploitée, cependant, un propriétaire devrait demander la localisation de ses appareils via l'application Find My, ont noté les chercheurs.

Une deuxième vulnérabilité pose un problème plus grave, ont constaté les chercheurs. Elle pourrait permettre à quelqu'un de construire « des applications macOS malveillantes pour récupérer et décrypter les rapports de localisation OF des sept derniers jours pour tous ses utilisateurs et pour tous leurs appareils ». L'équipe a partagé ses conclusions avec Apple et en réponse, l'entreprise a publié un correctif.

***Source***: *http://bit.ly/2OQSGdq*

## F5 Networks

### Bug critique F5 BIG-IP sous des attaques actives après un exploit PoC publié en ligne

20 mars 2021

Près de **10 jours** après que la firme de sécurité des applications F5 Networks ait publié des correctifs pour les vulnérabilités critiques de ses produits BIG-IP et BIG-IQ, les attaquants ont commencé à analyser et à cibler de manière opportuniste les périphériques réseau exposés et non corrigés pour pénétrer les réseaux d'entreprise.

La failles référencée CVE-2021-22986 affecte les versions 11.6 ou 12.x et plus récentes de BIG-IP, il s'agit d'une vulnérabilité d'exécution de commande à distance non authentifiée affectant l'interface iControl REST, permettant à un attaquant d'exécuter des commandes système arbitraires, de créer ou de supprimer des fichiers et de désactiver des services sans le besoin d'une authentification […].

Alors que F5 a déclaré qu'il n'était au courant d'aucune exploitation publique de ces problèmes le 10 mars, des chercheurs du groupe NCC ont déclaré qu'ils avaient maintenant trouvé des preuves d'une "exploitation complète de la chaîne de F5 BIG-IP / BIG-IQ iControl REST API vulnérabilités CVE-2021-22986 "à la suite de multiples tentatives d'exploitation contre son infrastructure de honeypot.

***Source :*** *http://bit.ly/3lzte8e*

# Actualité

## Les serveurs Microsoft Exchange font face au tsunami d'attaque APT

11 mars 2021

Microsoft a déclaré début mars avoir repéré plusieurs exploits zero-day utilisés pour attaquer des versions locales de Microsoft Exchange Server. Quatre failles peuvent être enchaînées pour créer un exploit d'exécution de code à distance (RCE) pré-authentification - ce qui signifie que les attaquants peuvent prendre le contrôle des serveurs sans connaître les informations d'identification de compte valides. Cela leur donne accès aux communications par e-mail et la possibilité d'installer une webshell pour une exploitation ultérieure dans l'environnement.

Microsoft a été incité à publier des correctifs hors bande pour les bugs exploités, connus collectivement sous le nom de ProxyLogon, référencées CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 et CVE-2021-27065.

Si elles sont utilisées conjointement, toutes ces vulnérabilités peuvent conduire à l'exécution de code à distance, à la compromission du serveur, à l'installation de portes dérobées, au vol de données et potentiellement à un déploiement ultérieur de logiciels malveillants.

Microsoft a demandé aux administrateurs et aux clients d'appliquer immédiatement les correctifs de sécurité. Toutefois, le fait que les correctifs soient appliqués maintenant ne signifie pas que les serveurs n'ont pas déjà été compromis auparavant. Des options alternatives sont également disponibles si l'application immédiate des correctifs n'est pas possible.

Le géant de Redmond a également publié un script sur GitHub, que les administrateurs informatiques peuvent utiliser et qui comprend des indicateurs de compromission (IOC) liés aux quatre vulnérabilités. Les IOC sont répertoriés séparément ici.

***Source*** *: http://bit.ly/3qNfLL7*

## Les systèmes Linux attaqués par un nouveau logiciel malveillant RedXOR

11 mars 2021

Les chercheurs ont découvert une nouvelle porte dérobée ciblant les systèmes Linux, qu'ils relient au groupe de menaces Winnti.

La porte dérobée est appelée RedXOR - en partie parce que son schéma de codage des données réseau est basé sur l'algorithme de chiffrement XOR, et en partie parce que ses exemples ont été trouvés sur une ancienne version de la plate-forme Red Hat Enterprise Linux. Ce dernier fait indique que RedXOR est utilisé dans des attaques ciblées contre les systèmes Linux hérités, d'après les chercheurs.

«Les systèmes Linux sont constamment attaqués étant donné que Linux fonctionne sur la majeure partie de la charge de travail du cloud public», ont déclaré les chercheurs d'Intezer. «Une enquête menée par Sophos a révélé que 70% des entreprises utilisant le cloud public pour héberger des données ou des charges de travail ont connu un incident de sécurité au cours de l'année écoulée.»

***Source*** *: http://bit.ly/38DLA6n*

## Google reCAPTCHA utilisé de manière abusive dans plusieurs campagnes de phishing

12 mars 2021

Plusieurs campagnes de phishing sur le thème de Microsoft ont été découvertes qui utilisent un faux Google reCAPTCHA. Dans ceux-ci, les attaquants recherchent les informations d'identification des employés supérieurs de diverses organisations. Selon le rapport de Zscaler, l'entreprise a arrêté plus de 2500 e-mails de phishing appartenant à cette campagne […].

Sur toute la durée, différents TLD ont été utilisés pour différentes campagnes d'attaque :

- **.xyz** TLD : dans cette campagne de phishing, les attaquants envoient un courrier indésirable qui semble provenir d'un système de communications unifiées et chargé d'un fichier HTML en pièce jointe, censé être un message vocal.
- **.club** TLD : elle suit le même schéma d'attaque que la campagne de phishing .xyz TLD ; Cependant, il utilise un faux Google reCAPTCHA, un écran de connexion Microsoft frauduleux, et se termine par montrer à l'utilisateur un fichier PDF hébergé.
- **.online** TLD : Dans cette campagne de phishing, les attaquants envoient un fichier PDF avec le lien de la campagne de phishing attaché, ainsi qu'une directive qui dit «REVIEW SECURE DOCUMENT» aux utilisateurs.

Ces campagnes d'attaque, destinées aux hauts dirigeants d'entreprise tels que les vice-présidents et les directeurs généraux, indiquent que les attaquants sont intéressés par des données sensibles qui nécessitent un niveau d'accès plus élevé. Pour se protéger contre de telles menaces, il est recommandé aux organisations de limiter l'accès à ces comptes et de mettre en œuvre une authentification à deux facteurs.

***Source*** *: http://bit.ly/30KnIWY*

## Des millions de personnes peuvent perdre des données sensibles grâce aux applications de voyage

18 mars 2021

Dans un rapport publié le 16 Mars par PrivacySavvy, de nombreuses entreprises de voyage exposent les données des utilisateurs à travers leurs applications de réservation […].

La plupart des applications de voyage populaires exposent leurs utilisateurs en permettant l'accès de tiers à leurs serveurs.

Puisqu'ils laissent ces serveurs ouverts, les données des utilisateurs sont exposées à toute personne intéressée par la collecte de ces données.

Les chercheurs n'ont pas divulgué les noms des applications de voyage spécifiques qu'ils ont testées en raison de problèmes juridiques et d'un possible compromis si des pirates informatiques accostaient de telles informations.

Selon les chercheurs de PrivacySavvy, tant les entreprises que les utilisateurs ont certains rôles dans la prévention de l'exposition des données.

Tout d'abord, les entreprises devraient :

1. Sécurisez à la fois leurs domaines principaux et leurs sous-domaines
2. Protéger les fichiers avec des informations sensibles
3. Ne jamais stocker de fichiers sur ses serveurs de production
4. Utilisation des règles d'accès appropriées
5. Arrêt des systèmes sans exigences d'authentification après utilisation

***Source :*** *https://bit.ly/3tGmDfg*

## Les utilisateurs du navigateur peuvent être suivis même lorsque JavaScript est désactivé

15 mars 2021

Selon un article académique, les acteurs de la menace peuvent lancer des attaques qui fuient des bouts d'informations depuis les navigateurs même lorsque JavaScript est complètement désactivé, ce qui permet un suivi secret même lorsque les utilisateurs peuvent penser qu'ils sont en sécurité.

Rédigé par une équipe d'universitaires américains, australiens…, le document de recherche a analysé l'état des attaques par canal auxiliaire pouvant être menées contre les navigateurs.

L'attaque par canal secondaire qui reposait uniquement sur du code HTML et CSS était capable de divulguer suffisamment de données des navigateurs des utilisateurs où JavaScript était entièrement désactivé - un conseil que les chercheurs en sécurité donnent souvent aux utilisateurs pour empêcher le suivi, les fuites et les attaques par canal secondaire.

L'équipe académique a déclaré avoir testé ses attaques non seulement contre les navigateurs fonctionnant sur des processeurs Intel, qui étaient le plus souvent montrés dans le passé comme étant vulnérables aux attaques par canal latéral, mais également contre les navigateurs fonctionnant sur des plates-formes de processeur telles que Samsung Exynos, AMD Ryzen. , et même la nouvelle puce M1 d'Apple - marquant la première fois connue qu'une attaque par canal latéral fonctionnait contre la nouvelle architecture de processeur d'Apple.

Dans une proposition du W3C ce mois-ci, les ingénieurs de Google prévoyaient que les attaques par canal secondaire évolueraient au-delà de JavaScript et seraient effectuées uniquement via CSS et ont exhorté les développeurs à changer la façon dont ils créent des sites Web et traitent les données, en fournissant plusieurs recommandations.

***Source :*** *https://bit.ly/3swZTOr*

## Comptes d'entreprise Instagram attaqués par CopperStealer

27 mars 2021

Les chercheurs de Proofpoint ont repéré et bloqué un voleur de cookies et de mots de passe. Nommé CopperStealer, ce malware serait dans la même classe que celui de SilentFade, Scranos, StressPaint et FacebookRobot.

Ce malware cible désormais les comptes professionnels Instagram et Facebook pour voler les mots de passe stockés dans Edge, Chrome, Opera, Firefox et Yandex. L'accès non autorisé a ensuite été utilisé par les opérateurs pour placer des publicités malveillantes sur les plateformes et en tirer profit.

CopperStealer n'est pas la seule menace qui plane sur les réseaux sociaux. En voici d'autres. Instagram a été témoin d'une augmentation de 50% des fraudes depuis le début de la pandémie. Les escroqueries qui figurent en tête du classement incluent les sponsors de romance, de phishing et d'influence.

**Gardez vos informations d'identification en sécurité.**

***Source :*** *https://bit.ly/2QKsjqm*

## Cette fausse mise à jour Android cache un dangereux malware, ne l'installez pas !

26 mars 2021

Les chercheurs en sécurité informatique de Zimperium ont découvert un nouveau malware particulièrement dangereux. Le maliciel en question se cache dans une appli baptisée "Mise à jour système". Une fois installé sur un smartphone, le logiciel malveillant est capable d'en prendre le contrôle pour voler un maximum de données […].

Cette application, introuvable sur le Play Store, peut être installée via un fichier APK. Une fois installé sur le smartphone de la victime, le malware est en mesure d'en prendre le contrôle, l'objectif étant de voler un maximum de données enregistrées sur l'appareil […].

Ce logiciel espion peut voler les messages, la liste des contacts, les détails de l'appareil, ou encore l'historique de navigation. Il peut même enregistrer les appels et capter des sons en activant le micro du smartphone. Cerise sur le gâteau, ce malware peut également déclencher l'appli photo à distance et prendre des clichés à l'insu de l'utilisateur.

Il convient d'éviter de télécharger des applications qui ne proviennent pas directement du Play Store.

***Source :*** *https://bit.ly/36hk4Ho*

# Evènements

## Evènements du mois

### Technologies de l'Information et de la Communication au MAGHREB

**15-17 Mars 2021, Alger, Algérie**

**https://bit.ly/3w5226e**

ICT MAGHREB 2021 est un Salon Professionnel sur les Technologies de l'information et de la communication réservé aux décideurs IT.

Dans sa première édition, l'événement a accueilli plus de 5.000 visiteurs professionnels et 150 exposants dont les principaux acteurs algériens du secteur des Technologies de l'Information ainsi que 40 % d'entreprises étrangères parmi lesquelles les grandes multinationales.

Plus de 30 conférences et ateliers ont été organisés sur trois jours suscitant un vif intérêt par le public. L'ANPT a participé à l'événement ICT Maghreb en tant qu'exposant et conférencier.

### Cyber Security & Cloud Expo Virtual

**17 -18 Mars 2021, Online**

**https://bit.ly/3ryafwn**

Le Cyber Security & Cloud Virtual Expo a été présenté dans une série de keynotes de haut niveau, de tables rondes interactives et d'études de cas basées sur des solutions, axées sur l'apprentissage et la création de partenariats dans le monde émergent de la cybersécurité et du cloud.

Les principaux sujets examinés sont les suivants : DevSecOps et sécurité des applications, sécurité et paysages du cloud, défense du réseau, gestion des risques, automatisation, technologies émergentes, sensibilisation et culture de la sécurité.

Cette conférence virtuelle s'est adressée aux professionnels ambitieux de la technologie d'entreprise, qui cherchent à explorer les dernières innovations, mises en œuvre et stratégies pour faire avancer les entreprises.

## Evènements à venir

### International Conference on Cryptography and Cloud Cybersecurity

**April 05-06, 2021 in Dubai, UAE**

**https://bit.ly/3csGvwy**

La Conférence internationale sur la recherche est une organisation fédérée qui se consacre à rassembler un nombre important d'événements universitaires divers pour une présentation dans le cadre du programme de la conférence

L'évènement vise à rassembler des scientifiques universitaires et des chercheurs de premier plan pour échanger et partager leurs expériences et leurs résultats de recherche sur tous les aspects de la cryptographie et de la cybersécurité dans le cloud. Il fournit également une plate-forme interdisciplinaire de premier ordre aux chercheurs, praticiens et éducateurs pour présenter et discuter des innovations, tendances et préoccupations les plus récentes, ainsi que des défis pratiques rencontrés et des solutions adoptées dans les domaines de la cryptographie et de la cybersécurité dans le cloud.

La conférence offre la possibilité de devenir un commanditaire ou un exposant de la conférence. Pour participer en tant que commanditaire ou exposant, veuillez télécharger et remplir le formulaire de demande de commandite de conférence .

| | |
|---|---|
| **Reference** | ANPT-2021-BV-03 |
| **Titre** | Bulletin de veille N°03 |
| **Date de version** | 31 Mars 2021 |
| **Contact** | ssi@anpt.dz |