
# BULLETIN DE VEILLE N°08

ANPT-2024-BV-08

**"Cybercrime is the greatest threat to every company in the world."**
**— Ginni Rometty**

Août 2024

# Alertes de sécurité

## SonicWall

### SonicWall corrige une faille critique affectant ses pare-feu (CVE-2024-40766)

26 Août 2024

SonicWall a corrigé une vulnérabilité critique (CVE-2024-40766) dans ses pares-feux de nouvelle génération qui pourrait permettre à des attaquants distants d'accéder sans autorisation à des ressources et, dans des conditions spécifiques, de faire planter les appareils.

CVE-2024-40766 est une vulnérabilité de contrôle d'accès incorrect dans « l'accès de gestion SonicWall SonicOS », indique la société.

« Ce problème affecte les pare-feu SonicWall Gen 5 et Gen 6, ainsi que les appareils Gen 7 fonctionnant sous SonicOS 7.0.1-5035 et les versions antérieures.

Des mises à jour de sécurité corrigeant la vulnérabilité sont disponibles pour tous les modèles de pare-feu next-gen actuellement pris en charge.

« Cette vulnérabilité n'est pas reproductible dans la version du micrologiciel SonicOS supérieure à 7.0.1-5035 », a indiqué la société, qui a néanmoins conseillé aux utilisateurs d'installer la dernière version du micrologiciel.

Bien qu'il soit préférable de passer à une version corrigée, il existe une alternative, c'est-à-dire une solution de contournement pour minimiser le potentiel d'exploitation : les utilisateurs peuvent restreindre l'accès à la gestion du pare-feu à des sources de confiance (par exemple, en établissant une liste blanche d'adresses IP spécifiques) ou désactiver l'accès à la gestion du réseau étendu du pare-feu à partir de sources Internet.

Les solutions de sécurité de SonicWall sont largement utilisées et parfois ciblées par des attaquants qui cherchent à pénétrer dans les réseaux d'entreprise.

En 2021, des chercheurs ont découvert que des attaquants avaient exploité des failles de type « zero-day » dans les appliances SonicWall Email Security, ainsi qu'une faille de type « zero-day » dans les appliances Secure Mobile Access (SMA) de la série 100 de l'entreprise.

Mais il n'y a actuellement aucune mention de l'exploitation de CVE-2024-40766

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

## Microsoft

### Mise à jour urgente de la sécurité Edge : Microsoft corrige des vulnérabilités de type Zero-day et RCE

26 Août 2024

Microsoft a publié une mise à jour de sécurité urgente pour son navigateur Edge, qui corrige une vulnérabilité critique actuellement exploitée par des acteurs malveillants. Cette faille, connue sous le nom de CVE-2024-7971, existe dans le moteur JavaScript V8 de Google Chrome et permet l'exécution de code à distance par le biais d'une page HTML malveillante.

La nouvelle version 128.0.2739.42 de Microsoft Edge Stable Channel, basée sur les versions 128.0.6613.85 et 128.0.6613.84 de Chromium, corrige un total de 25 vulnérabilités de sécurité. Vingt d'entre elles proviennent du projet Chromium, la CVE-2024-7971 étant la plus urgente en raison de son exploitation active dans la nature.

Outre les correctifs apportés par Chromium, la mise à jour résout cinq vulnérabilités propres à Microsoft Edge. Deux d'entre elles, CVE-2024-38209 et CVE-2024-38210, sont également capables de permettre l'exécution de code à distance et ont été classées comme « importantes », avec un score de base CVSSv3.1 de 7,8.

Le fait que la CVE-2024-7971 soit activement exploitée souligne l'urgence pour les utilisateurs de Edge d'installer immédiatement la dernière mise à jour. Les attaquants peuvent exploiter cette vulnérabilité pour obtenir un accès non autorisé aux systèmes, ce qui peut conduire au vol de données, à l'installation de logiciels malveillants ou à la prise de contrôle complète du système.

*Source* ***:https://bit.ly/47bUXDH***

# Actualité

**Une cyberattaque massive a touché la Banque centrale d'Iran et d'autres banques iraniennes**

Iran International rapporte qu'une cyberattaque massive a perturbé les opérations de la Banque centrale d'Iran (CBI) et de plusieurs autres banques du pays. L'attaque a paralysé les systèmes informatiques des banques du pays.

Cet incident coïncide avec l'intensification de la surveillance internationale des opérations de l'Iran au Moyen-Orient, Téhéran ayant annoncé des attaques contre Israël à moins d'un cessez-le-feu dans le conflit de Gaza. Les experts du renseignement accusent également l'Iran de tenter d'influencer les prochaines élections présidentielles américaines.

Selon Iran International, il s'agit de l'une des plus importantes cyberattaques contre l'infrastructure de l'État iranien à ce jour.

Plus tôt dans la journée de mercredi, le guide suprême iranien, l'ayatollah Ali Khamenei, a déclaré que « l'exagération des capacités de nos ennemis est destinée à répandre la peur parmi notre peuple par les États-Unis, la Grande-Bretagne et les sionistes. La main de l'ennemi n'est pas aussi forte qu'on le dit. Nous devons compter sur nous-mêmes. L'objectif de l'ennemi est de répandre la guerre psychologique pour nous faire reculer politiquement et économiquement et atteindre ses objectifs. »

« Cette cyberattaque survient à un moment où les actions de l'Iran dans la région font l'objet d'une surveillance internationale accrue, l'Iran ayant promis de riposter à l'assassinat du chef du Hamas, Ismail Haniyeh, au début du mois. Les dirigeants du Royaume-Uni, de la France et de l'Allemagne ont publié une déclaration commune avertissant l'Iran qu'il « portera la responsabilité » de toute attaque contre Israël, ce qui pourrait aggraver les tensions régionales et compromettre les efforts déployés en vue d'un cessez-le-feu et d'un accord sur la libération des otages », a rapporté le site web Hayom.

Les dirigeants européens ont exhorté l'Iran et ses alliés à éviter de nouvelles attaques afin d'éviter une nouvelle escalade entre Israël et le Hamas.

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

**Des espions russes ont piraté des données et des courriels du gouvernement britannique au début de l'année**

Au début de l'année, les services de renseignement étrangers russes ont volé des courriels internes et des données sur des individus au gouvernement britannique. La nouvelle a d'abord été rapportée par Recorded Future News, qui a obtenu une description officielle du rapport d'incident.

La description du rapport a été obtenue en vertu de la loi sur la liberté de l'information. Elle révèle que l'incident fait suite à une attaque menée par un acteur étatique sur un fournisseur des systèmes d'entreprise du ministère, et établit un lien entre la faille de sécurité et l'annonce faite par Microsoft en janvier.

En janvier, Microsoft a averti que certains de ses comptes de messagerie d'entreprise avaient été compromis par un groupe de cyber espionnage lié à la Russie et connu sous le nom de Midnight Blizzard. L'entreprise a informé les autorités chargées de l'application de la loi et les autorités réglementaires compétentes.

Microsoft a également annoncé que l'APT Midnight Blizzard, lié à la Russie, qui a frappé l'entreprise à la fin du mois de novembre 2023, ciblait des organisations du monde entier dans le cadre d'une campagne de cyber espionnage à grande échelle.

The Record Media suppose que les clients gouvernementaux de Microsoft ont pu découvrir qu'ils avaient été touchés par la violation des mois après que le géant de l'informatique a découvert l'attaque.

« Le lendemain du dépôt du rapport sur la violation des données auprès de l'autorité britannique de régulation de la protection des données, le Royaume-Uni et ses alliés ont publié une déclaration commune condamnant la cyber activité malveillante des services de renseignement russes - bien que cette déclaration se concentre spécifiquement sur l'activité d'une autre agence russe, le GRU, qui a été accusée d'avoir attaqué le Parti social-démocrate allemand », a rapporté The Record Media.

Microsoft a déclaré qu'il n'y avait aucune preuve que des systèmes en contact avec les clients hébergés par Microsoft aient été compromis à la suite de l'attaque divulguée en janvier.

« Nous n'avons trouvé aucune preuve que des systèmes clients hébergés par Microsoft aient été compromis à la suite de l'attaque contre Microsoft que nous avons révélée en janvier. Comme nous l'avions indiqué à l'époque, l'auteur de la menace n'a accédé qu'à un très faible pourcentage des comptes de messagerie d'entreprise de Microsoft », a déclaré un porte-parole de Microsoft à The Record. « Nous avons envoyé des notifications aux clients qui ont correspondu avec les comptes de messagerie d'entreprise Microsoft concernés.

***Source :*** ***https://bit.ly/3Z8xFq1***

# Bon à savoir

**Protégez votre information personnelle et rester en sécurité dans l'internet**

La cybersécurité est essentielle à l'ère numérique actuelle, et il existe plusieurs pratiques clés que tout le monde devrait connaître pour rester en sécurité en ligne.

Tout d'abord, il faut se méfier des attaques de phishing, qui sont des tentatives frauduleuses d'obtenir des informations sensibles par le biais de courriels ou de messages trompeurs. Ne cliquez jamais sur des liens suspects et ne téléchargez jamais de pièces jointes provenant de sources inconnues. L'activation de l'authentification à deux facteurs (2FA) ajoute une couche de sécurité supplémentaire à vos comptes en exigeant une deuxième forme de vérification en plus de votre mot de passe. Il est également essentiel d'utiliser des

mots de passe forts et uniques pour chacun de vos comptes ; ceux-ci doivent comporter un mélange de lettres, de chiffres et de caractères spéciaux afin d'être plus difficiles à deviner. La mise à jour régulière de vos logiciels, y compris votre système d'exploitation, vos applications et vos programmes antivirus, vous permet de vous protéger contre les dernières menaces et vulnérabilités. En outre, faites attention à ce que vous partagez sur les médias sociaux, car un partage excessif peut fournir aux cybercriminels des informations qu'ils peuvent utiliser pour deviner les mots de passe ou répondre aux questions de sécurité. Enfin, soyez conscient des risques liés aux réseaux Wi-Fi publics ; évitez d'accéder à des informations sensibles sur des réseaux publics ou utilisez un VPN pour crypter vos données et garantir la confidentialité.

# Evènements

## Evènement à venir

**Audit 403: Fraud Trends - Applying Real-Life Lessons**
**23 Sep 2024 - Online**
***https://bit.ly/3MpaRkO***

Fraud Trends Events se concentrera sur des exemples réels et pratiques de fraude dans des environnements de petite et moyenne taille, y compris les organisations à but non lucratif. La fraude implique un acte intentionnel de tromperie, qui peut entraîner des anomalies significatives dans les états financiers en raison d'une information financière frauduleuse ou d'un détournement d'actifs. La responsabilité de la direction est de concevoir, de mettre en œuvre, de maintenir et de surveiller un système de contrôle interne pour prévenir, ou détecter et corriger, la fraude. Note : Cette formation fait partie du programme de 16 heures proposé pour le niveau 4 des compétences en matière d'audit, destiné aux responsables expérimentés ou aux seniors. Cet événement peut être une rediffusion d'un événement en direct et l'instructeur sera disponible pour répondre à vos questions pendant l'événement.

| | |
|---|---|
| **Référence** | ANPT-2024-BV-08 |
| **Titre** | Bulletin de veille N°08 |
| **Date de version** | 31 août 2024 |
| **Contact** | ssi@anpt.dz |