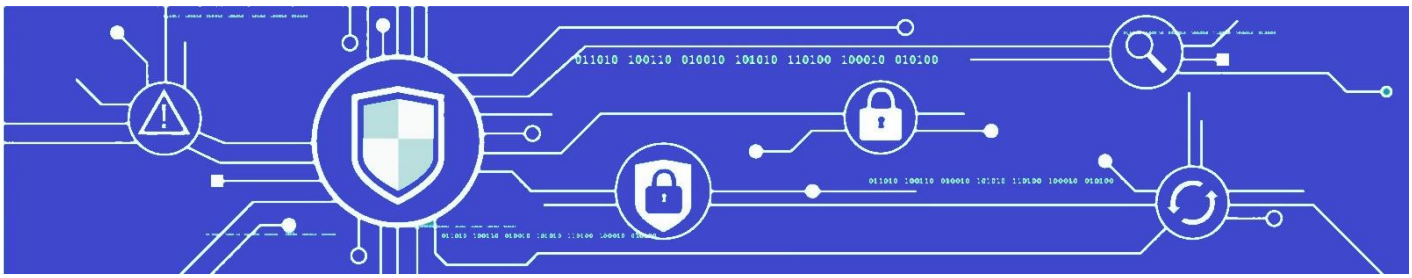

Vulnérabilités des pare-feu SonicWall avec SonicOS

Le fabricant SonicWall a publié un avis de sécurité (SNWLID-2025-0003) détaillant plusieurs vulnérabilités dans le logiciel SonicOS. Celles-ci concernent notamment le composant SSLVPN et la gestion SSH. Les attaquants pourraient exploiter ces vulnérabilités pour contourner les mécanismes d'authentification et établir des connexions non autorisées. Ces vulnérabilités affectent plusieurs modèles de pare-feu SonicWall et représentent un risque majeur pour la sécurité du réseau.

De quoi s'agit-il ?

Au total, quatre failles de sécurité ont été identifiées et seront corrigées par la mise à jour. Il s'agit notamment d'une vulnérabilité permettant de contourner l'authentification dans le VPN SSL et d'une faille permettant une escalade des droits d'utilisateur jusqu'à l'accès root dans les fonctions de configuration SSH. En outre, une Server-Side-Request-Forgery a été découverte dans la gestion SSH. Ces vulnérabilités représentent des risques importants pour la sécurité des systèmes concernés.

Détails des points faibles :

ID de conseil SNWLID-2025-0003
CVE CVE-2024-40762, CVE-2024-53704, CVE-2024-53705, CVE-2024-53706
CWE CWE-338, CWE-287, CWE-918, CWE-269
CVSS 8.2
CVSS Vec VSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

ID CVE	Produits concernés	Version corrigée
CVE-2024-40762	Série de pare-feu Gen6 et Gen7	7.0.1-5165 ou supérieur
CVE-2024-53704	Série de pare-feu Gen6 et Gen7	7.1.3-7015 ou supérieur
CVE-2024-53705	Pare-feu Gen6 et Gen7	7.0.1-5165 ou supérieur
CVE-2024-53706	Gen7 Cloud	7.1.3-7015 ou supérieur

Quel est le niveau de menace sur mon installation ?

Le niveau de menace est élevé. Les attaquants peuvent exploiter les failles de sécurité pour :

- de contourner les mécanismes d'authentification et d'obtenir un accès non autorisé aux systèmes.
- d'étendre les droits du système et d'obtenir un contrôle administratif.
- d'accéder à des zones sensibles de l'infrastructure et de lancer d'autres attaques.

Les systèmes particulièrement vulnérables sont ceux qui :

- Avoir un accès direct à Internet.
- ne pas avoir installé de mises à jour de sécurité récentes
- ne pas disposer de mécanismes de protection tels que l'authentification multi-facteurs

Comment puis-je m'en protéger ?

SonicWall a publié une mise à jour qui corrige les vulnérabilités identifiées.

Il est fortement recommandé d'installer cette mise à jour immédiatement afin de sécuriser vos systèmes.

Mettez à jour le firmware : Installez les mises à jour du micrologiciel fournies par Sonicwall afin de combler la faille de sécurité.

Activer l'authentification multi-facteurs
Protégez vos systèmes grâce au niveau de sécurité supplémentaire de l'authentification multifactorielle.

Pour obtenir de l'aide, vous pouvez contacter la ligne d'assistance payante au **0844 11 22 11**. Si vous utilisez le service de mise à jour, les frais ne sont pas facturés.

Service de mise à jour
Chaque système devrait être régulièrement mis à jour afin de le protéger contre les nouvelles vulnérabilités découvertes. Pour un pare-feu en particulier, nous vous recommandons une mise à jour régulière du logiciel, car il s'agit du composant de sécurité le plus important sur le périmètre du réseau pour la protection de votre réseau.

Avec notre service, nous garantissons que vos systèmes sont régulièrement contrôlés, optimisés et mis à jour. Ainsi, la sécurité de votre réseau reste toujours à la pointe du progrès.

Rittmeyer AG
6341 Baar, Suisse
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity

Publié : 09/01/2025