

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 27-07-2025

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans Sophos Firewall
Référence	1371
Date de Publication	2025-07-22
Sévérité	Critique

IMPACT :

- Exécution du code arbitraire à distance
- Injection SQL
- Injection des commandes systèmes
- Manipulation requêtes DNS

SYSTÈME AFFECTÉ :

- Sophos Firewall v21.0 GA (21.0.0) et version antérieure
- Sophos Firewall v21.5 GA (21.5.0) et version antérieure

DÉSCRIPTION :

Plusieurs vulnérabilités critiques ont été identifiées dans Sophos Firewall. Leur exploitation pouvait permettre à un attaquant, même sans authentification préalable, d'exécuter du code arbitraire à distance, d'écrire des fichiers arbitraires, d'injecter des commandes ou des requêtes SQL, ainsi que de manipuler des requêtes DNS.

SOLUTION :

Mettre à jour Sophos firewall. (se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Sophos du 21 Juillet 2025:

<https://www.sophos.com/fr-fr/security-advisories/sophos-sa-20250721-sfos-rce>

- CVE-2025-6704:<https://nvd.nist.gov/vuln/detail/CVE-2025-6704>
- CVE-2025-7624:<https://nvd.nist.gov/vuln/detail/CVE-2025-7624>
- CVE-2025-7382:<https://nvd.nist.gov/vuln/detail/CVE-2025-7382>
- CVE-2024-13974:<https://nvd.nist.gov/vuln/detail/CVE-2024-13974>
- CVE-2024-13973:<https://nvd.nist.gov/vuln/detail/CVE-2024-13973>