

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 03-02-2026

BULLETIN ALERTES

| | |
|---------------------|--|
| Object | Vulnérabilité dans les produits Fortinet |
| Référence | 1416 |
| Date de Publication | 2026-02-03 |
| Sévérité | Critique |

IMPACT :

- Contournement de la politique de sécurité

SYSTÈME AFFECTÉ :

- FortiAnalyzer versions 7.0.x antérieures à 7.0.16 (à venir)
- FortiAnalyzer versions 7.2.x antérieures à 7.2.12 (à venir)
- FortiAnalyzer versions 7.4.x antérieures à 7.4.10
- FortiAnalyzer versions 7.6.x antérieures à 7.6.6 (à venir)
- FortiManager versions 7.0.x antérieures à 7.0.16 (à venir)
- FortiManager versions 7.2.x antérieures à 7.2.13 (à venir)
- FortiManager versions 7.4.x antérieures à 7.4.10
- FortiManager versions 7.6.x antérieures à 7.6.6 (à venir)
- FortiOS versions 7.0.x antérieures à 7.0.19 (à venir)
- FortiOS versions 7.2.x antérieures à 7.2.13 (à venir)
- FortiOS versions 7.4.x antérieures à 7.4.11
- FortiOS versions 7.6.x antérieures à 7.6.6 (à venir)
- FortiProxy versions 7.6.x antérieures à 7.6.6 (à venir)
- FortiProxy versions antérieures à 7.4.13 (à venir)



DÉSCRIPTION :

Une vulnérabilité de **contournement de l'authentification** (CWE-288) a été découverte dans plusieurs produits **Fortinet** (FortiOS, FortiManager, FortiAnalyzer, FortiProxy et FortiWeb).

Elle permet à un attaquant disposant d'un **compte FortiCloud** et d'un **équipement enregistré** de se connecter à d'autres appareils enregistrés sous **d'autres comptes**, lorsque l'authentification **FortiCloud SSO** est activée.

SOLUTION :

Consulter le bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité Fortinet FG-IR-26-060 du 27 janvier 2026

<https://www.fortiguard.com/psirt/FG-IR-26-060>

- Référence CVE CVE-2026-24858

<https://www.cve.org/CVERecord?id=CVE-2026-24858>

