

**BULLETIN D'ALERTE**  
**N°0125-BA004****Vulnérabilité critique dans FortiSwitch**Origine : GN-CERT/ANSSI  
Date de l'alerte : 20/01/2025**ABSTRACT**

Le 20 janvier 2025, le GN-CERT a observé qu'une vulnérabilité critique a été découverte dans plusieurs des appareils Fortinet FortiSwitch.

Ce bulletin d'actualité présente les informations dont le **GN-CERT** à connaissance à ce jour concernant ces vulnérabilités.

**DESCRIPTION**

Une vulnérabilité critique CVE-2023-37936 a été découverte dans plusieurs versions de Fortinet Appareils FortiSwitch. Cette vulnérabilité, classée comme une utilisation de clé cryptographique codée en dur [CWE321], permet à un attaquant distant non authentifié en possession de la clé d'exécuter du code non autorisé via une requête cryptographique contrefaite.

- **CVE-2023-37936** : contournement de l'authentification dans le module websocket de FortiOS et FortiProxy
- **CWE-321** : Utilisation d'une clé cryptographique codée en dur
- **Gravité** : Score CVSSv3.1 **9.6 CRITIQUE, Très Urgent.**
- **Métrique** : CVSS :3.1/AV : N/AC : L/PR : N/UI : N/S : U/C :H/I :H/A :H
- **Score d'exploitabilité** : 3.9
- **Score d'impact** : 5.9

**VERSIONS AFFECTÉES**

- FortiSwitch 7.4.0
- FortiSwitch 7.2.0 à 7.2.5
- FortiSwitch 7.0.0 à 7.0.7
- FortiSwitch 6.4.0 à 6.4.13
- FortiSwitch 6.2.0 à 6.2.7
- FortiSwitch 6.0.0 à 6.0.7

**VERSIONS CORRIGÉES**

- FortiSwitch 7.4: Upgrade à to 7.4.1 ou supérieur
- FortiSwitch 7.2: Upgrade à 7.2.6 ou supérieur
- FortiSwitch 7.0: Upgrade à 7.0.8 ou supérieur
- FortiSwitch 6.4: Upgrade à 6.4.14 ou supérieur
- FortiSwitch 6.2: Upgrade à 6.2.8 ou supérieur
- FortiSwitch 6.0: Migrer vers une version fixe

## RISQUES

L'utilisation d'une clé cryptographique codée en dur dans Fortinet FortiSwitch versions 7.4.0 et 7.2.0 à 7.2.5 et 7.0.0 à 7.0.7 et 6.4.0 à 6.4.13 et 6.2.0 à 6.2.7 et 6.0.0 à 6.0.7 permet à l'attaquant d'exécuter du code ou des commandes non autorisés via des requêtes contrefaites.

## MESURES À PRENDRE

Le **GN-CERT** recommande de mettre à jour les versions du micrologiciel pour tous les équipements FortiSwitch concernés.

**Veillez diffuser ces informations à vos filiales et partenaires et partager avec nous toute information et constatation pertinente.**

## REFERENCES

- <https://fortiguard.fortinet.com/psirt/FG-IR-23-260>

## AUTRES LIENS POUR RESTER INFORME

- <https://www.facebook.com/ANSSIGN>
- <https://twitter.com/AnssiGuinee>

