



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
*Agence nationale de la sécurité
des systèmes d'information
CERT-FR*

Paris, le 18 août 2016
N° CERTFR-2016-AVI-283

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans le micrologiciel Fortigate de Fortinet

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTFR-2016-AVI-283 |
| Titre | Vulnérabilité dans le micrologiciel Fortigate de Fortinet |
| Date de la première version | 18 août 2016 |
| Date de la dernière version | 23 août 2016 |
| Source(s) | Bulletin de sécurité Fortinet FG-IR-16-023 du 17 août 2016 |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance

2 - Systèmes affectés

- FortiGate (FOS) versions antérieures à 4.3.9
- La migration vers une version 5.x de FortiGate (FOS) est cependant recommandée lorsque celle-ci est possible

3 - Résumé

Une vulnérabilité a été corrigée dans *le micrologiciel Fortigate de Fortinet*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Fortinet FG-IR-16-023 du 17 août 2016
<http://fortiguard.com/advisory/FG-IR-16-023>
- Règle de détection réseau Emerging Threats
<http://docs.emergingthreats.net/bin/view/Main/2023075>
- Référence CVE CVE-2016-6909
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6909>

Gestion détaillée du document

18 août 2016 version initiale.

23 août 2016 ajout CVE-2016-6909.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>

Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-283>
