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 26 décembre 2016
N° CERTFR-2016-ALE-010

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans les routeurs Netgear

Gestion du document

Référence	CERTFR-2016-ALE-010
Titre	Vulnérabilité dans les routeurs Netgear
Date de la première version	13 décembre 2016
Date de la dernière version	26 décembre 2016
Source(s)	Bulletin de sécurité Netgear du 09 décembre 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

- R6250
- R6400
- R6700
- R6900
- R7000
- R7100LG
- R7300DST
- R7900
- R8000
- D6220
- D6400

3 - Résumé

Une vulnérabilité a été découverte dans *les routeurs Netgear*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Description

Le 9 décembre 2016, Netgear a émis un avis de sécurité indiquant que plusieurs de ses routeurs étaient vulnérables à une injection de commande à distance.
Un attaquant non authentifié peut exploiter cette vulnérabilité à distance si l'utilisateur se rend sur un site piégé.
Cela lui permet alors d'exécuter des commandes arbitraires avec les privilèges les plus élevés (`root`).
A noter qu'un attaquant présent sur le réseau local peut directement exploiter cette vulnérabilité.

Depuis le 24 décembre 2016, un correctif de sécurité est disponible pour le micrologiciel de chaque modèle vulnérable.

5 - Solution

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

6 - Documentation

- Avis CERT-FR CERTFR-2016-AVI-430 Routeurs Netgear
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-430/index.html
- Bulletin de sécurité Netgear du 09 décembre 2016
  http://kb.netgear.com/000036386/CVE-2016-582384
- CERT Carnegie Mellon
  https://www.kb.cert.org/vuls/id/582384
- Référence CVE CVE-2016-6277
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6277

Gestion détaillée du document

13 décembre 2016 version initiale.

26 décembre 2016 mise à jour de la liste des systèmes affectés et clôture de l'alerte.