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 11 avril 2016
N° CERTFR-2015-ALE-014-1

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Juniper ScreenOS

Gestion du document

Référence	CERTFR-2015-ALE-014
Titre	Vulnérabilité dans Juniper ScreenOS
Date de la première version	18 décembre 2015
Date de la dernière version	11 avril 2016
Source(s)	Bulletin de sécurité Juniper SA10713 du 17 décembre 2015
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)

– contournement de la politique de sécurité

2 - Systèmes affectés

– Juniper ScreenOS versions 6.3.0r12 à 6.3.0r20
– Juniper ScreenOS versions 6.2.0r15 à 6.2.0r18

3 - Résumé

Une vulnérabilité a été découverte dans *Juniper ScreenOS*. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité.

4 - Solution

Une mise à jour de sécurité a été publiée hier sur le site officiel de Juniper.

Cette mise à jour corrige plusieurs failles de sécurité critiques au niveau du système ScreenOS, identifiées à la suite d'un audit de code interne réalisé par Juniper.

La première vulnérabilité corrigée permettait à un attaquant de se connecter, via les protocoles SSH ou telnet, à tout équipement réseau Juniper utilisant une version vulnérable du système d'exploitation ScreenOS (versions antérieures à 6.2.0r18 ou 6.3.0r20).

De plus, le mot de passe de la porte dérobée a été identifié et a été rendu public sur Internet.

Cette compromission peut être détectée par la présence dans les journaux de notifications de connexions "anormales" pendant lesquelles le passage en mode administrateur (system) s'effectue depuis un compte utilisateur "standard" (username2) :

```
    2015-12-17 09:00:00 system warn 00515 Admin user system has logged on
via SSH from [...]
    2015-12-17 09:00:00 system warn 00528 SSH: Password authentication
successful for admin user 'username2' at host [...]
```

Cependant la société Juniper souligne le fait qu'un attaquant, ayant le niveau requis pour exploiter cette vulnérabilité, aura vraisemblablement effacé toute trace de ses connexions dans les journaux.

La société Fox-It propose des signatures au format Snort afin d'identifer toute tentative de connexion à un équipement Juniper vulnérable via la porte dérobée.

La seconde vulnérabilité permettait à un attaquant, en capacité d'écouter le trafic VPN émis depuis un équipement concerné, de déchiffrer ce trafic.

Le CERT-FR recommande donc aux utilisateur de Juniper ScreenOS de procéder à une mise à jour immédiate du système d'exploitation. De plus, le CERT-FR insiste sur l'importance d'isoler l'accès aux interfaces d'administration des équipements réseaux afin de n'autoriser que les connexions depuis des systèmes de confiance.

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

5 - Documentation

- Bulletin de sécurité Juniper SA10713 du 17 décembre 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST
- Règles Snort de détection d'exploitation
  https://gist.github.com/fox-srt/ca94b350f2a91bd8ed3f
- Référence CVE CVE-2015-7755
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7755
- Référence CVE CVE-2015-7756
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7756
- Annonce Juniper
  http://forums.juniper.net/t5/Security-Incident-Response/Juniper-Networks-Completes-ScreenOS-Update/ba-p/290368
- ScreenOS 6.3.0r22
  http://www.juniper.net/support/downloads/screenos.html
- CERTFR-2016-AVI-117
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-117/

Gestion détaillée du document

18 décembre 2015 version initiale.

21 décembre 2015 ajout de règles Snort dans les contournements provisoires.

11 avril 2016 clôture de l'alerte