



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 09 juillet 2008
N° CERTA-2008-AVI-360

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'implémentation du protocole DNS par Juniper

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-360>

Gestion du document

Référence	CERTA-2008-AVI-360
Titre	Vulnérabilité dans l'implémentation du protocole DNS par Juniper
Date de la première version	09 juillet 2008
Date de la dernière version	–
Source(s)	Alerte AL-2008.0080 de l'AusCERT du 09 juillet 2008
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Juniper Firewall sous ScreenOS ;
- Juniper J-Series Routers sous JUNOS, version antérieure au 23 Mai 2008 ;
- Juniper switches sous JUNOS, version antérieure au 23 Mai 2008.

3 Résumé

Une vulnérabilité a été découverte dans l'interprétation du protocole DNS par certains produits Juniper. Cette vulnérabilité peut être exploitée afin de corrompre le cache d'un serveur.

4 Description

Une vulnérabilité a été découverte dans plusieurs produits Juniper. Cette vulnérabilité résulte d'une mauvaise implémentation dans le traitement du protocole et permet à un utilisateur malintentionné de corrompre le cache d'un serveur présentant cette faiblesse.

Des outils permettant l'exploitation de cette vulnérabilité ont été rendus publiques.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Des identifiants sont nécessaires pour accéder à la page. Contactez votre support officiel.

6 Documentation

- Alerte de l'AusCERT AL-2008.0080 du 09 juillet 2008 :
<http://www.auscert.org.au/render.html?it=9546>
- Bulletin de mise à jour Juniper PSN-2008-06-040 :
<http://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2008-06-040&viewMode=view>
- Référence CVE CVE-2008-1447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447>
- Référence CVE CVE-2008-1454 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1454>

Gestion détaillée du document

09 juillet 2008 version initiale.