Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 février 2013
N° CERTA-2009-ALE-017-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans l'implémentation TCP/IP de divers produits

Gestion du document

Référence	CERTA-2009-ALE-017-003
Titre	Vulnérabilités dans l'implémentation TCP/IP de divers produits
Date de la première version	09 septembre 2009
Date de la dernière version	19 février 2013
Source(s)	
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

Déni de service à distance.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Red Hat Enterprise Linux 3, 4, 5 ;
- Red Hat Enterprise MRG ;
- Sun Solaris versions 8, 9 et 10.

D'autres produits sont très probablement affectés par ces vulnérabilités.

3 Résumé

Des vulnérabilités dans la pile TCP/IP de certains produits permettent à une personne malintentionnée distante de provoquer un déni de service.

4 Description

Plusieurs vulnérabilités dans l'implémentation TCP/IP de certains produits permettent à une personne malintentionnée distante de provoquer un déni de service. Les conséquences, failles et le volume de trafic nécessaire peuvent varier selon les produits.

Microsoft a annoncé ne pas corriger ces failles pour Windows 2000, qui bénéficie officiellement d'un support étendu jusqu'au 13 juillet 2010.

Microsoft n'a également pas publié de correctif pour Windows XP car la configuration par défaut n'est pas affectée (pas d'exception dans le pare-feu intégré).

5 Contournement provisoire

Les personnes utilisant l'un des systèmes concernés comme poste client peuvent utiliser un dispositif de filtrage à état (*stateful*) afin de bloquer les connexions entrantes non sollicitées.

Au besoin, les utilisateurs sont invités à lire les bulletins de sécurité des différents éditeurs pour des contournements adaptés aux produits concernés.

6 Solution

Les vulnérabilités ont été corrigés dans les produits Microsoft (MS09-048), Oracle (CPUJul2012), Redhat (RHBA-2009-1539), Solaris (Sun Alert 267088) et Cisco (cisco-sa-20090908-tcp24). Se rapprocher de l'éditeur pour obtenir un correctif pour les produits non cités.

7 Documentation

- Bulletin de sécurité Microsoft MS09-048 du 08 septembre 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-048.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx
- Bulletin de sécurité Oracle CPUJul2012 de juillet 2012 :
  http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
- Bulletin de sécurité Redhat RHBA-2009-1539 du 02 octobre 2009 :
  https://rhn.redhat.com/errata/RHBA-2009-1539.html
- Bulletin de sécurité Cisco cisco-sa-20090908-tcp24 du 08 septembre 2009 :
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24
- Entrée 18730 de la base de connaissances de Red Hat :
  http://kbase.redhat.com/faq/docs/DOC-18730
- Avis de sécurité du CERT-FI :
  http://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html
- Bulletin de sécurité Sun Solaris Alert 267088 du 09 septembre 2009 :
  http://download.oracle.com/sunalerts/1020909.1.html
- Référence CVE CVE-2008-4609 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609
- Référence CVE CVE-2009-1926 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1926

Gestion détaillée du document

09 septembre 2009 version initiale ;

09 septembre 2009 modification de l'alerte pour prendre en compte tous les produits ;

11 septembre 2009 ajout du bulletin de sécurité Sun Solaris.

19 février 2013 fermeture de l'alerte.