

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

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

---

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-2009-ALE-017>

---

### Gestion du document

Référence	CERTA-2009-ALE-017-002
Titre	Vulnérabilités dans l'implémentation TCP/IP de divers produits
Date de la première version	09 septembre 2009
Date de la dernière version	11 septembre 2009
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).

L'éditeur Red Hat a annoncé ne pas publier de correctif pour ses produits. Un contournement permettant de limiter les effets a été publié sur leur site (cf. section Documentation).

## 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 Documentation

- Bulletin de sécurité Microsoft MS09-048 du 08 septembre 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-048.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-048.msp>
- 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 #267088 du 09 septembre 2009 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-267088-1>
- 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.