



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 avril 2005
N° CERTA-2005-AVI-135

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le traitement des paquets ICMP

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-2005-AVI-135>

Gestion du document

Référence	CERTA-2005-AVI-135
Titre	Vulnérabilités dans le traitement des paquets ICMP
Date de la première version	13 avril 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité NISCC du 12 avril 2005
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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 3 et Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) et Service Pack 1 (Itanium) ;
- Microsoft Windows 2003 Server (x86 et Itanium) ;
- Microsoft Windows 98, 98 Second Edition (SE) et Millenium Edition (ME) ;
- tous les produits Cisco basés sur Cisco IOS (toutes versions) avec PMTUD activé ;
- les produits Cisco suivants non basés sur Cisco IOS : Cisco CRS-1, Cisco PIX Security Appliance, Cisco IP Phones, Cisco Catalyst 6608 Voice Gateway et Cisco 6000 FXS Analog Interface Module, Cisco 11000 et 11500 Content Service Switches, Global Site Selector, Cisco ONS products, Cisco MDS 9000 Series Multilayer Switches, VPN 5000 concentrator ;
- Sun Solaris 7, 8, 9 et 10 pour les plates-formes x86 et SPARC.

3 Résumé

Plusieurs vulnérabilités dans le traitement des paquets ICMP permettent à un utilisateur mal intentionné de réaliser un déni de service sur la plate-forme vulnérable.

4 Description

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer des informations de contrôle relatives aux machines connectées.

Trois types d'attaques utilisant des paquets ICMP malicieusement construits permettent à un utilisateur mal intentionné de réaliser des dénis de service sur la plate-forme vulnérable : arrêt à distance d'une connexion TCP, diminution à distance des performances d'une connexion TCP ou consommation excessive des ressources processeur et mémoire.

5 Solution

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

6 Documentation

- Bulletin de sécurité NISCC 532967/NISCC/ICMP du 12 avril 2005 :
<http://www.niscc.gov.uk/niscc/docs/al-20050412-00308.html>
- Bulletin de sécurité de l'US-CERT VU#222750 :
<http://www.kb.cert.org/vuls/id/222750>
- Bulletin de sécurité Microsoft MS05-019 du 12 avril 2005 :
<http://www.microsoft.com/technet/security/bulletin/ms05-019.msp>
- Bulletin de sécurité Cisco #64520 du 12 avril 2005 :
<http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>
- Bulletin de sécurité Sun #57746 du 12 avril 2005 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1>
- Papier expliquant les attaques ICMP sur le site Internet de l'IETF :
<http://www.ietf.org/internet-drafts/draft-gont-tcpm-icmp-attacks-03.txt>
- Référence CVE CAN-2004-790 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0790>
- Référence CVE CAN-2004-791 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0791>

Gestion détaillée du document

13 avril 2005 version initiale.