



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 avril 2004
N° CERTA-2004-AVI-114

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PERL WIN32

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-2004-AVI-114>

Gestion du document

Référence	CERTA-2004-AVI-114
Titre	Vulnérabilité dans PERL WIN32
Date de la première version	08 avril 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDEFENSE
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

PERL WIN32 versions 5.8.3 et antérieures.

3 Résumé

Une vulnérabilité dans la fonction win32_stat de PERL WIN32 permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine cible.

4 Description

L'envoi d'une requête HTTP judicieusement composée vers un serveur utilisant la fonction win32_stat permet, par le biais d'un débordement de mémoire, d'exécuter du code arbitraire à distance.

5 Solution

- La version 5.8.4 de PERL corrigera cette vulnérabilité ;
- Correctif pour la version PERL 5.8.x :
<http://public.activestate.com/cgi-bin/perlbrowse?patch=22552>
- Correctif pour la version PERL 5.9.x en développement :
<http://public.activestate.com/cgi-bin/perlbrowse?patch=22466>

6 Documentation

- Bulletin de sécurité de iDEFENSE 04.05.04 :
<http://www.odefense.com/application/poi/display?id=93&type=vulnerabilities>
- Référence CVE CAN-2004-0377 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0377>

Gestion détaillée du document

08 avril 2004 version initiale.