



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juillet 2003
N° CERTA-2003-AVI-123

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les serveurs Novell Netware

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-2003-AVI-123>

Gestion du document

Référence	CERTA-2003-AVI-123
Titre	Vulnérabilité dans les serveurs Novell Netware
Date de la première version	25 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité Novell VU#185593 du CERT/CC
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 ;
- Déni de service.

2 Systèmes affectés

Serveurs Novell Netware 5.1 et 6.

3 Résumé

Un utilisateur distant mal intentionné peut, par le biais d'une requête HTTP judicieusement composée, exécuter du code arbitraire sur le serveur vulnérable ou réaliser un déni de service.

4 Description

Une vulnérabilité a été découverte dans l'interpréteur PERL du serveur Web de Novell (Netware Enterprise Web Server).

Une mauvaise gestion des requêtes HTTP à destination de l'interpréteur PERL par le module CGI2PERL.NLM peut entraîner un débordement de pile, permettant à un utilisateur distant de réaliser un déni de service, voire l'exécution de code arbitraire avec les privilèges du serveur web (Admin).

5 Solution

Appliquer le correctif disponible sur le site de l'éditeur :
<http://support.novell.com/servlet/filedownload/ftf/cgiperl71903.exe>

6 Documentation

Bulletin de sécurité Novell :
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966549.htm>
Note du CERT CC :
<http://www.kb.cert.org/vuls/id/185593>
Référence CVE CAN-2003-0562 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0562>

Gestion détaillée du document

25 juillet 2003 version initiale.