



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2002
N° CERTA-2002-AVI-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Netscape Enterprise Server et iPlanet Web Server

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-2002-AVI-005>

Gestion du document

Référence	CERTA-2002-AVI-005
Titre	Multiples vulnérabilités dans Netscape Enterprise Server et iPlanet Web Server
Date de la première version	14 janvier 2002
Date de la dernière version	–
Source(s)	Bulletins de sécurité PR01-04 et PR01-05 de ProCheckUp
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 ;
- divulgation d'informations.

2 Systèmes affectés

Netscape Enterprise Server 3.x et iPlanet Web Server 4.x.

Ces produits sont disponibles sur de nombreuses plate-formes : Solaris, AIX, Digital Unix, HP-UX, IRIX, SunOS, Windows NT, Windows 2000, Linux.

3 Résumé

Netscape Enterprise Server et iPlanet Web Server utilisent un module appelé Web Publisher permettant aux utilisateurs d'accéder, d'éditer et de gérer des fichiers résidants sur un serveur web distant.

Deux vulnérabilités présentes dans Web Publisher permettent à un utilisateur mal intentionné de découvrir les mots de passe des utilisateurs ou de réaliser un déni de service sur le serveur web.

4 Description

4.1 Déni de service

Au moyen d'une commande `?wp-html-rend` habilement constituée, un utilisateur mal intentionné peut provoquer l'arrêt à distance du serveur web. Le service doit alors être redémarré manuellement.

Cette vulnérabilité n'est exploitable que sur les plate-formes Windows.

4.2 Divulgarion d'informations

La commande `wp-force-auth` de Web Publisher permet d'initier une séquence d'authentification (avec une en-tête `HTTP Authorization:Basic`) même si aucun document sur le serveur n'est protégé par un mot de passe.

En utilisant plusieurs commandes `wp-force-auth`, un utilisateur mal intentionné peut réaliser une attaque de type "force brute" sur les mots de passe utilisés par des comptes bien identifiés tels que `nobody`, `root` sur un système Unix.

5 Contournement provisoire

Pour déterminer si le service Web Publishing est activé, on utilisera l'url suivante :

`http://<nom-du-serveur>/publisher.`

Il est conseillé de ne pas démarrer ce service sur les serveurs Web externes :

`http://developer.netscape.com/docs/manuals/enterprise/40/ag/esapuirf.htm#1005372`

6 Solution

Se référer aux articles #7761 et #7764 de la base de connaissances iPlanet.

7 Documentation

- Netscape Enterprise Server Administrator's guide - configuring Web Publishing :
`http://developer.netscape.com/docs/manuals/enterprise/40/ag/eswebpub.htm`
- article #7761 de la base de connaissances iPlanet "`?wp-html-rend causes access violation on Windows NT and 2000`" :
`http://knowledgebase.iplanet.com/ikb/kb/articles/7761.html`
- article #7764 de la base de connaissances iPlanet "`?wp-force-auth can be used in a brute force password cracking attack`" :
`http://knowledgebase.iplanet.com/ikb/kb/articles/7764.html`
- bulletin de sécurité PR01-04 de ProCheckUp "`Netscape ?wp-html-rend denial of service attack`" :
`http://www.procheckup.com/vulnerabilities/pr0104.html`
- bulletin de sécurité PR01-05 de ProCheckUp "`Netscape publishing wp-force-auth`" :
`http://www.procheckup.com/vulnerabilities/pr0105.html`
- bulletin de sécurité VU#191763 du CERT/CC "`iPlanet Web Server Enterprise Edition and Netscape Enterprise Server malformed Web Publisher command causes denial-of-service`" :
`http://www.kb.cert.org/vuls/id/191763`
- bulletin de sécurité VU#985347 du CERT/CC "`iPlanet Web Server Enterprise Edition and Netscape Enterprise Server Web Publisher command exposes server to brute force attack`" :
`http://www.kb.cert.org/vuls/id/985347`

Gestion détaillée du document

14 janvier 2002 version initiale.