



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 novembre 2008
N° CERTA-2008-AVI-566

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans HP Secure Web Server et Internet Express

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-2008-AVI-566>

Gestion du document

Référence	CERTA-2008-AVI-566
Titre	Vulnérabilité dans HP Secure Web Server et Internet Express
Date de la première version	26 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP c01599836 du 25 novembre 2008
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 ;
- déni de service à distance.

2 Systèmes affectés

- HP Secure Web Server version 6.8.0 pour Tru64 UNIX et les versions précédentes ;
- HP Internet Express version 6.6 pour Tru64 UNIX ;
- HP Internet Express version 6.7 pour Tru64 UNIX ;
- HP Internet Express version 6.8 pour Tru64 UNIX.

3 Résumé

Une vulnérabilité affecte les produits HP Web Secure Server et HP Internet Express et permet à une personne distante malintentionnée d'effectuer un déni de service ou d'exécuter du code arbitraire.

4 Description

Un dépassement de mémoire tampon dans la fonction *imagerloadfont* de *gd.c* permet à une personne distante malintentionnée d'effectuer un déni de service ou d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Bulletin de sécurité HP c01599836 du 25 novembre 2008 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01599836>
- Référence CVE CVE-2008-3658 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3658>

Gestion détaillée du document

26 novembre 2008 version initiale.