Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 octobre 2011
N° CERTA-2011-AVI-607

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Fujitsu Interstage HTTP Server

Gestion du document

Référence	CERTA-2011-AVI-607
Titre	Vulnérabilités dans Fujitsu Interstage HTTP Server
Date de la première version	31 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Fujitsu 201104eN du 31 octobre 2011
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 à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Interstage Application Server versions 5.x, 6.x, 7.x, 8.x et 9.x ;
- Interstage Apworks versions 6.x et 7.x ;
- Interstage Business Application Server versions 8.x ;
- Interstage Job Workload Server versions 8.x ;
- Interstage Studio versions 8.x et 9.x.

3 Résumé

Deux vulnérabilités ont été signalées dans Interstage HTTP Server, qui peuvent être exploitées pour créer un déni de service ou contourner la politique de sécurité.

4 Description

Deux vulnérabilités ont été signalées dans Interstage HTTP Server. La première peut être exploitée par un attaquant distant à l'aide d'une requête à distance spécialement conçue, qui provoque une occupation importante du processeur et donc un déni de service. La seconde peut être exploitée pour atteindre un hôte protégé par le serveur proxy inverse (reverse proxy), à l'aide d'une requête à distance spécialement conçue.

Ces vulnérabilités n'existent que dans certaines configurations du serveur (fichier httpd.conf).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour les solutions de contournement (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Fujitsu 201104eN du 31 octobre 2011 :
  http://www.fujitsu.com/global/support/software/security/products-f/interstage-201104e.html
- Référence CVE CVE-2011-3368 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368

Gestion détaillée du document

31 octobre 2011 version initiale.