Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 novembre 2011
N° CERTA-2011-AVI-663

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Tomcat pour HP-UX

Gestion du document

Référence	CERTA-2011-AVI-663
Titre	Vulnérabilités dans HP-UX Tomcat Servlet Engine
Date de la première version	24 novembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP c03090723 du 21 novembre 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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

HP-UX Apache Web Server Suite version 3.19 et antérieures.

3 Résumé

De multiples vulnérabilités permettant de contouner la politique de sécurité, porter atteinte à la confidentialité et à l'intégrité des données, effectuer un déni de service ou injecter du code à distance sont présentes dans *HP-UX Tomcat Servlet Engine*.

4 Description

Plusieurs vulnérabilités sont présentes dans le module *HP-UX Tomcat Servlet Engine* embarqué dans *HP-UX Apache Web Server Suite*. Ces vulnérabilités permettent à un utilisateur distant malintentionné de :

- contourner la politique de sécurité (CVE-2011-2526, CVE-2011-2729, CVE-2011-3190) ;
- effectuer un déni de service à distance (CVE-2010-4476, CVE-2011-2526) ;
- porter atteinte à la confidentialité des données (CVE-2010-3718, CVE-2011-2204) ;
- porter atteinte à l'intégrité des données (CVE-2010-3718) ;
- injecter indirectement du code à distance (CVE-2011-0013).

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 c03090723 du 21 novembre 2011 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03090723
- Référence CVE CVE-2010-3718 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3718
- Référence CVE CVE-2010-4476 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4476
- Référence CVE CVE-2011-0013 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0013
- Référence CVE CVE-2011-2204 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2204
- Référence CVE CVE-2011-2526 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2526
- Référence CVE CVE-2011-2729 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2729
- Référence CVE CVE-2011-3190 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3190

Gestion détaillée du document

24 novembre 2011 version initiale.