



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2008
N° CERTA-2008-AVI-397

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cygwin

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-397>

Gestion du document

Référence	CERTA-2008-AVI-397
Titre	Vulnérabilités dans Cygwin
Date de la première version	12 août 2008
Date de la dernière version	–
Source(s)	Annnonce de Security Objectives SECOBJADV-2008-02 du 25 juillet 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

- Contournement de la politique de sécurité ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Les versions antérieures à 2.573.2.3.

3 Résumé

Des vulnérabilités ont été identifiées dans l'application Cygwin. L'une d'elles, en particulier, permet à une personne malveillante d'exécuter sous certaines conditions du code arbitraire sur un système vulnérable.

4 Description

Des vulnérabilités ont été identifiées dans l'application Cygwin. L'application ne vérifie pas correctement l'identité du serveur de téléchargement, permettant ainsi à une personne malveillante de faire télécharger sous certaines conditions une application non légitime sur le système.

5 Solution

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

6 Documentation

- Annonce de changement de version Cygwin du 05 août 2008 :
<http://cygwin.com/ml/cygwin-announce/2008-08/msg00001.html>
- Avis de sécurité de Security Objectives SECOBJADV-2008-02 du 25 juillet 2008 :
<http://www.security-objectives.com/advisories/SECOBJADV-2008-02.txt>
- Site de téléchargement de la dernière version de Cygwin :
<http://cygwin.com/setup/snapshots/setup-2.573.2.3.exe>
- Référence CVE CVE-2008-3323 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3323>

Gestion détaillée du document

12 août 2008 version initiale.