Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 novembre 2007
N° CERTA-2007-AVI-485

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Mono

Gestion du document

Référence	CERTA-2007-AVI-485
Titre	Vulnérabilités dans Mono
Date de la première version	08 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mono
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- *Mono* versions 1.2.5.1 et antérieures pour Windows (CVE-2007-5473);
- *Mono* versions antérieures à 1.2.5.1 (CVE-2007-5197).

3 Résumé

Deux vulnérabilités ont été découvertes dans *Mono* permettant d'exécuter du code arbitraire et d'atteindre à la confidentialité des données.

4 Description

Deux failles ont été découvertes dans *Mono* :

- la première vulnérabilité affecte toutes les versions 1.x (antérieures à 1.2.5.1) de *Mono*. Elle permet l'exécution de code arbitraire (CVE-2007-5197) ;
- la seconde vulnérabilité n'affecte que les versions 1.x (antérieures à 1.2.5.2) pour Windows de *Mono*. Elle permet d'accéder au code source de certains fichiers (CVE-2007-5473).

5 Solution

Installer la version 1.2.5.1 ou la version 1.2.5.2 selon la plate-forme utilisée (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Mono :
  http://www.mono-project.com/Vulnerabilities#BigInteger_unsafe_code_overflow
- Téléchargement de Mono :
  http://www.mono-project.com/Downloads
- Bulletin de sécurité Debian DSA 1397 du 03 novembre 2007 :
  http://www.debian.org/security/2007/dsa-1397
- Bulletin de sécurité Gentoo GLSA-200711-10 du 07 novembre 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200711-10.xml
- Référence CVE CVE-2007-5197 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5197
- Référence CVE CVE-2007-5473 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5473

Gestion détaillée du document

08 novembre 2007 version initiale.