



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 07 juillet 2004  
N° CERTA-2004-AVI-182-004

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Tripwire

---

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-2004-AVI-182>

---

### Gestion du document

Référence	CERTA-2004-AVI-182-004
Titre	Vulnérabilité de Tripwire
Date de la première version	07 juin 2004
Date de la dernière version	07 juillet 2004
Source(s)	Avis de sécurité Gentoo GLSA 200406-02
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.

## 2 Systèmes affectés

- Pour la version commerciale de Tripwire : toutes les versions antérieures à la version 4.0.1 ;
- pour la version open source de Tripwire : toutes les versions antérieures à la version 2.3.1.

## 3 Résumé

Un débordement de mémoire dans le logiciel Tripwire permet à un utilisateur mal intentionné de faire exécuter du code arbitraire sur la machine cible.

## 4 Description

Tripwire est un logiciel utilisé pour le contrôle d'intégrité d'un système. Il est disponible en version commerciale et en version open source. Il est possible de réaliser un débordement de mémoire lorsque Tripwire envoie un

résumé sous forme de message électronique. En créant un fichier habilement constitué, un utilisateur mal intentionné peut faire exécuter du code arbitraire avec les permissions de l'utilisateur exécutant Tripwire (qui peut être l'utilisateur `root`).

## 5 Solution

Se référer à la section Documentation pour l'obtention du correctif.

## 6 Documentation

- Site Internet de la version commerciale de Tripwire :  
<http://www.tripwire.com>
- Site Internet de la version open source de Tripwire :  
<http://www.tripwire.org>
- Avis de sécurité Gentoo GLSA 200406-02 du 04 juin 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200406-02.xml>
- Bulletin de sécurité MDKSA-2004:057 de Mandrake du 07 juin 2004 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:057>
- Bulletin de sécurité MDKSA-2004:057-1 de Mandrake du 07 juillet 2004 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:057-1>
- Avis de sécurité SUSE SuSE-SA:2004:015 du 09 juin 2004 :  
[http://www.suse.com/de/security/2004\\_15\\_cvs.html](http://www.suse.com/de/security/2004_15_cvs.html)
- Avis de sécurité RedHat RHSA-2004:244 du 15 juin 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-244.html>
- Référence CVE CAN-2004-0536 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0536>

## Gestion détaillée du document

**07 juin 2004** version initiale.

**08 juin 2004** ajout de la référence au bulletin de sécurité de Mandrake. Ajout référence CVE.

**09 juin 2004** ajout de la référence au bulletin de sécurité de SUSE.

**15 juin 2004** ajout de la référence au bulletin de sécurité de RedHat.

**07 juillet 2004** ajout de la référence au second bulletin de sécurité de Mandrake.