

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilité dans heimdal heimdal telnetd server

---

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-2005-AVI-239>

---

### Gestion du document

Référence	CERTA-2005-AVI-239-002
Titre	Multiples vulnérabilité dans heimdal telnetd server
Date de la première version	30 juin 2005
Date de la dernière version	18 juillet 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200506-24 du 29 juin 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

Toutes les versions antérieures à heimdal v0.6.5.

## 3 Résumé

De nombreuses vulnérabilités dans heimdal telnetd server permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

heimdal est une mise en oeuvre de Kerberos 5 pour les systèmes Linux. De nombreuses vulnérabilités de type débordement de mémoire affectent l'utilitaire heimdal telnetd server. Une personne distante mal intentionnée peut exploiter ces vulnérabilités pour exécuter du code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité de l'éditeur :  
<http://www.pdc.kth.se/heimdal/advisory/2005-06-20>
- Bulletin de sécurité Gentoo SA 200506-24 du 29 juin 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200506-24.xml>
- Bulletin de sécurité SUSE SUSE-SA:2005:040 du 06 juillet 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_40\\_heimdal.html](http://www.novell.com/linux/security/advisories/2005_40_heimdal.html)
- Bulletin de sécurité Debian DSA-758 du 18 juillet 2005 :  
<http://www.debian.org/security/2005/dsa-758>
- Référence CVE CAN-2005-2040 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2040>

## Gestion détaillée du document

**30 juin 2005** version initiale.

**06 juillet 2005** ajout de la référence au bulletin de sécurité SUSE SUSE-SA:2005:040.

**18 juillet 2005** ajout de la référence au bulletin de sécurité Debian DSA-758.