



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 septembre 2004  
N° CERTA-2004-AVI-299

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de xv

---

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-299>

---

### Gestion du document

Référence	CERTA-2004-AVI-299
Titre	Vulnérabilité de xv
Date de la première version	06 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA 200409-07 du 03 septembre 2004
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 ;
- exécution de code arbitraire.

## 2 Systèmes affectés

xv version 3.10a et versions antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans xv permettent à un utilisateur mal intentionné de créer un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

xv est un outil de manipulation d'images dans de nombreux formats. Plusieurs débordements de mémoire dans la partie de code réalisant le traitement des images permettent à un utilisateur mal intentionné, via l'envoi d'une image malicieusement constituée, de créer un déni de service ou d'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

- Site Internet de xv :  
<http://www.trilon.com/xv/>
- Bulletin de sécurité Gentoo GLSA 200409-07 du 03 septembre 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200409-07.xml>
- Référence CVE CAN-2004-0802 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0802>

## Gestion détaillée du document

**06 septembre 2004** version initiale.