



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2005
N° CERTA-2005-AVI-027-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Konversation

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-027>

Gestion du document

Référence	CERTA-2005-AVI-027-002
Titre	Vulnérabilité de Konversation
Date de la première version	24 janvier 2005
Date de la dernière version	14 février 2005
Source(s)	Bulletin de sécurité KDE du 21 janvier 2005
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 ;
- déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de Konversation antérieures à la version 0.15.1.

3 Description

Konversation est un client IRC (Internet Relay Chat) pour l'environnement de bureau KDE. Plusieurs vulnérabilités dans Konversation rendent possible le déni de service ou l'exécution de code arbitraire à distance sur la plate-forme utilisant une version non corrigée de Konversation.

4 Solution

Mettre à jour `Konversation` en version 0.15.1 (cf. section Documentation).
`Konversation` est téléchargeable à l'adresse suivante :
<http://download.berlios.de/konversation/>

5 Documentation

- Site Internet de `Konversation` :
<http://konversation.berlios.de>
- Bulletin de sécurité de Wouter Coekaerts :
<http://wouter.coekaerts.be/konversation.html>
- Bulletin de sécurité KDE du 21 janvier 2005 :
<http://www.kde.org/info/security/advisory-20050121-1.txt>
- Bulletin de sécurité Gentoo GLSA 200501-34 du 24 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-34.xml>
- Bulletin de sécurité SUSE-SR:2005:004 du 11 février 2005 :
http://www.novell.com/linux/security/advisories/2005_04_sr.html
- Référence CVE CAN-2005-0129 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0129>
- Référence CVE CAN-2005-0130 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0130>
- Référence CVE CAN-2005-0131 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0131>

Gestion détaillée du document

24 janvier 2005 version initiale.

25 janvier 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200501-34.

14 février 2005 ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:004.