



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 janvier 2004
N° CERTA-2004-AVI-011

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur de news INN d'ISC

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-011>

Gestion du document

Référence	CERTA-2004-AVI-011
Titre	Vulnérabilité du serveur de news INN d'ISC
Date de la première version	16 janvier 2004
Date de la dernière version	-
Source(s)	Note VU#759020 du CERT/CC Avis de sécurité SSA:2004-014-02 de slackware
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 à distance.

2 Systèmes affectés

INN version 2.4.0.

3 Résumé

Une vulnérabilité présente dans le serveur de news `innnd` livré avec le paquetage INN (InterNetNews) d'ISC (Internet Software Consortium) peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans la routine `ARTpost()` du serveur de news `innnd`.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité à distance afin d'exécuter du code arbitraire sur la plate-forme vulnérable avec les privilèges du service `inn.d`.

5 Solution

La version 2.4.1 de INN corrige cette vulnérabilité.

6 Documentation

- Internet Software Consortium :
<http://www.isc.org/products/INN>
- Note VU#759020 du CERT/CC :
<http://www.kb.cert.org/vuls/id/759020>
- Avis de sécurité SSA:2004-014-02 de slackware :
<http://www.securityfocus.com/advisories/6244>

Gestion détaillée du document

16 janvier 2004 version initiale.