

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Pidgin

---

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-2011-AVI-466>

---

### Gestion du document

Référence	CERTA-2011-AVI-466
Titre	Vulnérabilités dans Pidgin
Date de la première version	24 août 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Pidgin du 20 août 2011
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 à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

*Pidgin* versions antérieures à 2.10.0.

## 3 Résumé

Des vulnérabilités dans *Pidgin* permettent notamment de réaliser un déni de service à distance.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans *Pidgin* :

- certains caractères spécifiques utilisés dans les pseudonymes IRC peuvent provoquer un arrêt inopiné du client *Pidgin* lors des requêtes WHO ;

- une mauvaise gestion des réponses HTTP 100 via le protocole MSN peut provoquer une tentative d'accès à une zone non autorisée de la mémoire ;
- sous Windows, en cliquant sur un lien de type `file:///` reçu par message instantané, le client *Pidgin* tente d'exécuter le fichier.

## 5 Solution

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

## 6 Documentation

- Bulletins de sécurité Pidgin du 20 août 2011 :
  - <http://pidgin.im/news/security/?id=53>
  - <http://pidgin.im/news/security/?id=54>
  - <http://pidgin.im/news/security/?id=55>
- Référence CVE CVE-2011-2943 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2943>
- Référence CVE CVE-2011-3184 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3184>
- Référence CVE CVE-2011-3185 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3185>

## Gestion détaillée du document

**24 août 2011** version initiale.