

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de gestionnaire de contenu Zope

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-469>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-AVI-469 |
| Titre | Vulnérabilité de gestionnaire de contenu Zope |
| Date de la première version | 24 novembre 2005 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Zope |
| 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

Zope versions 2.7.4+ à 2.8.1.

3 Résumé

Certaines fonctionnalités peuvent être exploitées par un utilisateur mal intentionné pour insérer des pages dynamiques quelconques et donc exécuter du code arbitraire.

4 Description

Zope est une solution de gestion de contenu.

L'accès d'un utilisateur quelconque aux fonctionnalités de Zope nommées « RestructuredText » lui permet d'injecter du code quelconque.

5 Solution

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

6 Documentation

- Site internet de Zope :
<http://www.zope.org>
- Bulletin de sécurité Zope du 09 octobre 2005 :
http://www.zope.org/Products/Zope/Hotfix_2005-10-09/security_alert
- Bulletin de sécurité Debian DSA 910 du 24 novembre 2005 :
<http://www.debian.org/security/2005/dsa-910>
- Bulletin de sécurité Gentoo GLSA-200510-20 du 25 octobre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200510-20.xml>
- Bulletin de sécurité SUSE SuSE-SR:2005-027 du 11 novembre 2005 :
http://www.novell.com/linux/security/advisories/2005_27_sr.html
- Référence CVE CAN-2005-3323 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3323>

Gestion détaillée du document

24 novembre 2005 version initiale.