Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2001
N° CERTA-2001-AVI-115-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faille de sécurité dans Zope

Gestion du document

Référence	CERTA-2001-AVI-115-001
Titre	Faille de sécurité dans Zope
Date de la première version	12 octobre 2001
Date de la dernière version	19 octobre 2001
Source(s)	Avis de sécurité de l'éditeur
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Contournement de la politique de sécurité.

2 Systèmes affectés

Tout Unix , Windows 9x, NT incluant une version de Zope depuis la 2.2.0 jusqu'à la 2.4.1.

3 Résumé

Un utilisateur légitime de Zope peut, par le biais de pages *DTML* mal formées, accéder à des méthodes qui lui sont en principe inacessibles.

4 Description

Zope est une boîte à outils de gestion/création de portails ou sites "web" dynamiques. Elle inclut nativement un modèle de sécurité et utilise un langage de création de pages dynamiques proche du *HTML*, le *DTML*.

Les versions depuis la 2.2.0 jusqu'à la 2.4.1, n'effectuent pas de contrôle de sécurité sur l'attribut *fmt* (attribut de mise en forme d'une balise) de la balise d'inclusion de variables <*dtml-var*>. Un utilisateur mal intentionné peut alors utiliser cette faiblesse pour accéder à des méthodes qui lui sont normalement interdites.

5 Solution

- Pour Red Hat Powertools 6.2, 7.0 et 7.1, utiliser *up2date* ou télécharger les RPMs depuis :
  http://www.redhat.com/mailing-lists/linux-security/msg00043.html
- Pour Mandrake 7.1, 7.2 et Corporate Server 1.0.1, utiliser *MandrakeUpdate* ou télécharger les RPMs depuis :
  http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-080.php3
- Télécharger et installer le correctif de l'éditeur (instructions d'installation présentes) depuis :
  http://www.zope.org/Products/Zope/Products/Zope/Hotfix_2001-09-28/Hotfix_2001-09-28.tgz/view

6 Documentation

- Avis de sécurité de l'éditeur
  http://www.zope.org/Products/Zope/Hotfix_2001-09-28/security_alert
- Bulletin de sécurité Red Hat
  http://www.redhat.com/mailing-lists/linux-security/msg00043.html

Gestion détaillée du document

12 octobre 2001 version initiale.
19 octobre 2001 rajout de la distribution Linux Mandrake.