

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Python 2.2 : Débordement de variable dans la gestion des réponses du DNS

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-076>

Gestion du document

Référence	CERTA-2004-AVI-076-001
Titre	Python 2.2 : Débordement de variable dans la gestion des réponses du DNS
Date de la première version	10 mars 2004
Date de la dernière version	03 septembre 2004
Source(s)	CVE CAN-2004-150 Avis Mandrake : MDKSA-2004:019 Debian Security Advisory DSA 458-1
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.

2 Systèmes affectés

Les versions de 2.2 à 2.2.2 incluse de Python configurées sans la prise en compte du protocole IPv6.

3 Description

Python est un langage de programmation interprété, interactif et orienté objet. Dans l'environnement Unix, il est utilisé pour programmer de nombreuses applications.

Les versions 2.2 à 2.2.2 de Python, lorsqu'elles sont configurées pour ne pas prendre en compte le protocole IPv6, présentent une faille de sécurité dans la fonction `getaddrinfo`.

Un utilisateur distant mal intentionné peut exploiter cette faille pour confectionner une réponse de DNS malicieuse qui, lorsqu'elle est interprétée par une des versions vulnérables de Python, peut mener à l'exécution de code arbitraire.

Les versions de Python antérieures à 2.2 et à partir de 2.2.3 ne sont pas vulnérables à cette faille de sécurité.

4 Solution

Appliquer le correctif de sécurité. La distribution Debian a fourni un correctif de sécurité : Python 2.2 dans la version 2.2.1-4.3. La distribution Mandrake a fourni un correctif de sécurité : Python 2.2 dans la version 2.2.1-14.4.

Si l'éditeur de votre système d'exploitation n'a pas encore fourni un correctif « clef en main » pour une version vulnérable de Python 2.2, il est possible de compiler une version de Python supérieure ou égale à 2.2.3 à partir des sources.

5 Documentation

- Site Internet officiel du projet Python (téléchargement) :
<http://www.python.org/download/>
- Bulletin de sécurité Debian DSA-458 du 09 mars 2004 :
<http://www.debian.org/security/2004/dsa-458>
- Bulletin de sécurité Mandrake MDKSA-2004:019 du 09 mars 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:019>
- Bulletin de sécurité Gentoo GLSA 200409-03 du 02 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-03.xml>
- Mise à jour de sécurité du paquetage NetBSD python22 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/lang/python22/README.html>
- Référence CVE CAN-2004-0150 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0150>

Gestion détaillée du document

10 mars 2004 version initiale.

03 septembre 2004 ajout des références aux bulletins de sécurité Gentoo et NetBSD.