

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Xmail

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-496>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2005-AVI-496 |
| Titre | Vulnérabilité de Xmail |
| Date de la première version | 21 décembre 2005 |
| Date de la dernière version | – |
| Source(s) | Gentoo : GLSA 200512-05 CVE : CAN-2005-2943 Debian : DSA-902-1 |

TAB. 1 – *Gestion du document*

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

1 Risque

- Exécution de code arbitraire ;
- élévation de privilèges.

2 Systèmes affectés

Les versions de Xmail antérieures à 1.22.

Se reporter au bulletin des vendeurs pour la liste exhaustive des versions affectées connues.

3 Description

Xmail est un serveur qui met en œuvre les protocoles ESMTTP et POP3.

Cette application a une vulnérabilité de type débordement de variable. Cette vulnérabilité permettrait l'exécution de code malveillant avec les droits du groupe mail.

Le savoir-faire pour exploiter cette vulnérabilité a été publié. Il suffit de soumettre à Xmail une adresse de messagerie astucieusement construite.

4 Solution

Appliquer le correctif. La version 1.22 de Xmail corrige cette vulnérabilité. Des mises à jours spécifiques sous forme de paquets sont fournies par les différents vendeurs de distributions.

5 Documentation

- CVE :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2943> ;
- Avis de sécurité Debian :
<http://www.debian.org/security/2005/dsa-902> ;
- Avis Gentoo :
<http://www.gentoo.com/security/en/glsa/glsa-200512-05.xml>

Gestion détaillée du document

21 décembre 2005 version initiale.