

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des clients de messagerie Sylpheed et Sylpheed-Claws

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-452>

Gestion du document

Référence	CERTA-2005-AVI-452-002
Titre	Vulnérabilité des clients de messagerie Sylpheed et Sylpheed-Claws
Date de la première version	10 novembre 2005
Date de la dernière version	23 novembre 2005
Source(s)	
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 avec les privilèges de l'utilisateur courant.

2 Systèmes affectés

Tout système Unix ou Windows utilisant un client de messagerie :

- Sylpheed antérieur aux versions stables 2.0.4 ou 1.0.6 et de développement 2.1.6,
- Sylpheed-Claws en version antérieure à la 1.9.100.

3 Résumé

L'importation d'un carnet d'adresse au format d'échange LDIF (« Lightweight Directory Interchange Format ») malicieusement construit, présente un risque d'exécution de code arbitraire.

4 Description

Sylpheed et Sylpheed-Claws sont des clients de messagerie utilisant la boîte à outils graphique GTK+ et disponible sur Unix et Windows.

LDIF est un format de fichier texte permettant l'échange et la synchronisation de données entre serveurs d'annuaire LDAP. Ce format est donc employé pour l'échange de carnets d'adresses par certains clients de messagerie (Thunderbird, Evolution, Messenger, Outlook, Kmail, ...).

Des erreurs dans le code de Sylpheed et Sylpheed-Claws induisent un risque d'exécution de code.

5 Solution

Mettre à jour les versions source :

- Sylpheed versions stables 2.0.4 ou 1.0.6 au moins et version de développement 2.1.6 au moins,
- Sylpheed-Claws version 1.9.100 au moins.

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

6 Documentation

- Site internet de Sylpheed :
<http://sylpheed.good-day.net/en/>
- Site internet de Sylpheed-Claws :
<http://sylpheed-claws.sourceforge.net>
- Bulletin de sécurité Fedora Core 3 du 09 novembre 2005 :
<http://www.redhat.com/archives/fedora-announce-list/2005-November/msg00025.html>
- Bulletin de sécurité Gentoo GLSA 200511-13 du 15 novembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200511-13.xml>
- Bulletin de sécurité Debian DSA-906 du 22 novembre 2005 :
<http://www.debian.org/security/2005/dsa-906>
- Bulletin de sécurité Debian DSA-908 du 22 novembre 2005 :
<http://www.debian.org/security/2005/dsa-908>
- Référence CVE CVE-2005-3354 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3354>

Gestion détaillée du document

10 novembre 2005 version initiale.

21 novembre 2005 ajout de la référence au bulletin de sécurité Gentoo.

23 novembre 2005 ajout des références aux bulletins de sécurité Debian DSA-906 et DSA-908.