Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2005
N° CERTA-2005-AVI-180-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Qpopper

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-180

Gestion du document

Référence	CERTA-2005-AVI-180-002
Titre	Vulnérabilités dans Qpopper
Date de la première version	27 mai 2005
Date de la dernière version	21 novembre 2005
Source(s)	Avis de sécurité Debian DSA-728-2 Avis de sécurité Gentoo GLSA 200505-17
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

Elévation de privilèges.

2 Systèmes affectés

- Pour Debian 3.0 (woody), toutes les versions de Qpopper antérieures à la version 4.0.4-2.woody.5 sont vulnérables ;
- pour les autres distributions, toutes les versions de Qpopper antérieures à la version 4.0.5-r3 sont vulnérables.

3 Description

Deux vulnérabilités ont été découvertes dans Qpopper, qui est un serveur POP3.
Elles permettent à un utilisateur local mal intentionné d'augmenter ses privilèges.

4 Solution

Mettre à jour Qpopper dans la dernière version :
- pour Debian 3.0, il s'agit de la version 4.0.4-2.woody.5 ;

– pour les autres distributions, il s'agit de la version 4.0.5-r3.

5 Documentation

– Bulletin de sécurité Debian DSA-728-2 :
http://www.debian.org/security/2005/dsa-728
– Bulletin de sécurité Gentoo GLSA 200505-17/Qpopper du 23 mai 2005 :
http://www.gentoo.org/security/en/glsa/glsa-200505-17.xml
– Bulletin de sécurité SUSE SUSE-SR:2005:014 du 07 juin 2005 :
http://www.novell.com/linux/security/advisories/2005_14_sr.html
– Bulletin de sécurité FreeBSD pour qpopper du 07 novembre 2005 :
http://www.vuxml.org/freebsd/pkg-qpopper.html
– Référence CVE CAN-2005-1151
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1151
– Référence CVE CAN-2005-1152
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1152

Gestion détaillée du document

27 mai 2005 version initiale.
08 juin 2005 ajout référence au bulletin de sécurité SUSE.
21 novembre 2005 ajout référence au bulletin de sécurité FreeBSD.