

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2003-AVI-042>

Gestion du document

Référence	CERTA-2003-AVI-042-001
Titre	Vulnérabilité de qpopper
Date de la première version	13 mars 2003
Date de la dernière version	24 mars 2003
Source(s)	Avis de sécurité Debian DSA-259-1
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

- Elévation de privilèges ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de qpopper de la série 4.0.x antérieures à la version 4.0.4-9. Pour Debian 3.0 (woody), toutes les versions de qpopper de la série 4.0.x antérieures à la version 4.0.4-2.woody.3.

3 Résumé

Une vulnérabilité dans qpopper permet à un utilisateur possédant un compte sur la machine d'augmenter ses privilèges, d'obtenir un shell ou d'exécuter du code à distance avec les privilèges de l'utilisateur `mail`.

4 Description

qpopper est un serveur POP3 (Post Office Protocol) développé par Qualcomm. Une vulnérabilité dans la fonction `Qvsnprintf()` permet à un utilisateur possédant un compte sur la machine d'obtenir un shell ou d'exécuter du code à distance avec les privilèges de l'utilisateur `mail`.

5 Solution

Pour la Debian 3.0 (woody), mettre à jour qpopper en version 4.0.4-2.woody.3. Sinon, mettre à jour qpopper en version 4.0.4-9.

6 Documentation

- Site internet de qpopper :
<http://www.eudora.com/qpopper/>
- Avis de sécurité Debian DSA-259-1 :
<http://www.debian.org/security/>
- Bulletin de sécurité SuSE-SA:2003:018 de SuSE :
http://www.suse.com/de/security/2003_018_qpopper.html
- Référence CVE CAN-2003-0143 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0143>

Gestion détaillée du document

13 mars 2003 version initiale.

24 mars 2003 Ajout référence au bulletin de SuSE. Ajout référence CVE.