

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Courier MTA, Courier-IMAP et Courier SqWebMail

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-252>

Gestion du document

Référence	CERTA-2004-AVI-252
Titre	Vulnérabilité de Courier MTA, Courier-IMAP et Courier SqWebMail
Date de la première version	23 juillet 2004
Date de la dernière version	–
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

- Cross-site Scripting ;
- déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Courier MTA versions antérieures à la version 0.45 ;
- Courier-IMAP versions antérieures à la version 3.0.0 ;
- Courier SqWebMail version 4.0.4 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans Courier MTA, Courier-IMAP et Courier SqWebMail permettent à un utilisateur mal intentionné de réaliser de l'injection de données, réaliser un déni de service ou exécuter du code arbitraire à distance.

4 Description

Courier MTA (Mail Transfer Agent) est un serveur de messagerie. Courier-IMAP est un serveur IMAP (Internet Message Access Protocol). Courier SqWebMail est un module de type webmail pour le serveur de messagerie Courier MTA. Plusieurs vulnérabilités ont été identifiées Courier MTA, Courier-IMAP et Courier SqWebMail :

- Plusieurs débordements de mémoire dans Courier MTA, Courier-IMAP et Courier SqWebMail (CVE CAN-2004-0224) ;
- une vulnérabilité de type Cross-site Scripting dans la fonction `print_header_uc` de Courier SqWebMail (CVE CAN-2004-0591) ;

Ces vulnérabilités permettent à un utilisateur mal intentionné de réaliser de l'injection de données, réaliser un déni de service ou exécuter du code arbitraire à distance.

5 Solution

- Mettre à jour Courier MTA en version 0.45 ou supérieure ;
- Mettre à jour Courier-IMAP en version 3.0.0 ou supérieure ;
- Mettre à jour Courier SqWebMail en version 4.0.5 ou supérieure.
- A partir des sources :
<http://www.courier-mta.org/download.php>
- Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de Courier MTA, Courier-IMAP et Courier SqWebMail :
<http://www.courier-mta.org>
- Bulletin de sécurité Gentoo GLSA 200403-06 du 26 mars 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200403-06.xml>
- Bulletin de sécurité Debian DSA-533 du 22 juillet 2004 :
<http://www.debian.org/security/2004/dsa-533>
- Mise à jour de sécurité des paquetages NetBSD courier-auth, courier-imap et sqwebmail :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/courier-auth/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/courier-imap/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/sqwebmail/README.html>
- Référence CVE CAN-2004-0224 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0224>
- Référence CVE CAN-2004-0591 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0591>

Gestion détaillée du document

23 juillet 2004 version initiale.