



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2005
N° CERTA-2005-AVI-268-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Shorewall

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-268>

Gestion du document

Référence	CERTA-2005-AVI-268-003
Titre	Vulnérabilité de Shorewall
Date de la première version	18 juillet 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletin de sécurité Shorewall du 17 juillet 2005
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Shorewall version 2.4.1 et antérieures ;
- Shorewall version 2.2.5 et antérieures ;
- Shorewall version 2.0.17 et antérieures.

3 Résumé

Une vulnérabilité dans Shorewall permet à un utilisateur distant de contourner la politique de sécurité du système.

4 Description

Shorewall est un outil de configuration haut niveau du firewall GNU/Linux Netfilter. Une vulnérabilité dans la façon dont Shorewall gère l'authentification par adresse MAC (Medium Access Control) permet à un utilisateur mal intentionné du réseau local de contourner la politique de sécurité du système.

5 Solution

Mettre à jour avec les scripts corrigés de Shorewall disponibles aux adresses suivantes :

- Shorewall version 2.4.1 et antérieures :
<http://shorewall.net/pub/shorewall/2.4/shorewall-2.4.1/errata/firewall>
- Shorewall version 2.2.5 et antérieures :
<http://shorewall.net/pub/shorewall/2.2/shorewall-2.2.5/errata/firewall>
- Shorewall version 2.0.17 et antérieures :
<http://shorewall.net/pub/shorewall/errata/2.0.17/firewall>

6 Documentation

- Site de Shorewall :
<http://shorewall.net>
- Bulletin de sécurité Shorewall du 17 juillet 2005 :
<http://shorewall.net/News.htm#20050717>
- Bulletin de sécurité Mandriva MDKSA-2005:123 du 20 juillet 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:123>
- Bulletin de sécurité Gentoo GLSA 200507-20 du 22 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-20.xml>
- Bulletin de sécurité Debian DSA-849 du 08 octobre 2005 :
<http://www.debian.org/security/2005/dsa-849>
- Référence CVE CAN-2005-2317 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2317>

Gestion détaillée du document

18 juillet 2005 version initiale.

21 juillet 2005 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:123 et ajout de la référence CVE CAN-2005-2317.

22 juillet 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-20.

10 octobre 2005 ajout de la référence au bulletin de sécurité Debian DSA-849.