

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans SSH Secure Shell 3.0.0

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-2001-AVI-079>

Gestion du document

Référence	CERTA-2001-AVI-079
Titre	Vulnérabilité dans SSH Secure Shell 3.0.0
Date de la première version	24 juillet 2001
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

- Accès non autorisés ;
- Compromission de la machine.

2 Systèmes affectés

Version 3.0.0 de SSH Secure Shell sur les systèmes suivants :

- Red Hat Linux versions 6.1 à 7.1 incluses ;
- Solaris versions 2.6 à 2.8 incluses ;
- HP-UX versions 10.20 et 11.00 ;
- Caldera Linux version 2.4 ;
- SuSE Linux versions 6.4 à 7.0 incluses.

Notons que la version 3.0.0 de SSH Secure Shell n'est pas installée par défaut sur ces systèmes.

3 Résumé

Un utilisateur mal intentionné peut exploiter une vulnérabilité dans le système d'authentification pour se connecter sans mot de passe sur un compte.

4 Description

Lors de l'authentification par mot de passe, si le mot de passe contenu dans le fichier `/etc/passwd` ou `/etc/shadow` n'est composé que de 2 caractères ou moins, n'importe quel utilisateur pourra se connecter sur ce compte sans mot de passe.

Cette vulnérabilité est due à un bogue dans la partie du code qui effectue la comparaison entre le résultat de la fonction `crypt(mot_de_passe, salt)` et le mot de passe chiffré. La fonction `crypt()` renvoie une chaîne de 13 caractères, dont les 2 premiers sont le "salt". La comparaison est ensuite faite entre les n premiers caractères de la chaîne et le mot de passe chiffré, n étant le nombre de caractères du mot de passe chiffré (2 dans notre cas). Or la valeur choisie pour le "salt" par la fonction `crypt()` sont les deux premiers caractères du mot de passe chiffré.

La correspondance des 2 chaînes est donc toujours vérifiée.

5 Contournement provisoire

N'autoriser l'accès au démon `sshd2` qu'aux utilisateurs dont le mot de passe chiffré dans `/etc/passwd` ou `/etc/shadow` excède 2 caractères.

6 Solution

Mettre à jour SSH Secure Shell et installer la version 3.0.1. Cette version est disponible sur le site FTP de SSH :

`ftp://ftp.ssh.com/pub/ssh/`

7 Documentation

L'avis de sécurité de SSH :

`http://www.ssh.com/products/ssh/exploits.cfm`

Gestion détaillée du document

24 juillet 2001 version initiale.