

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'authentification OPIE dans FreeBSD

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-2006-AVI-126>

Gestion du document

Référence	CERTA-2006-AVI-126
Titre	Vulnérabilité de l'authentification OPIE dans FreeBSD
Date de la première version	23 mars 2006
Date de la dernière version	-
Source(s)	Bulletin de sécurité FreeBSD FreeBSD-SA-06:12.opie du 22 mars 2006
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 ;
- élévation de privilèges.

2 Systèmes affectés

Toutes les versions de FreeBSD.

3 Résumé

Une vulnérabilité dans un mécanisme d'authentification sous FreeBSD permet à un utilisateur mal intentionné d'élever ses privilèges.

4 Description

OPIE (One-time Passwords In Everything) est une mise en œuvre du système OTP (One-Time Password), un système basé sur des mots de passe dits jetables permettant de se prémunir contre les attaques par rejeu. Le programme `opiepasswd` est utilisé afin de contrôler l'authentification OPIE pour un utilisateur.

Sous FreeBSD, le mécanisme OPIE est activé par défaut au travers de PAM (Pluggable Authentication Module). Une vulnérabilité dans ce mécanisme d'authentification OPIE permet à un utilisateur mal intentionné, dans certaines conditions, d'élever ses privilèges.

5 Contournement provisoire

- Désactiver l'authentification par OPIE à travers PAM. Pour ceci, on pourra exécuter la commande :

```
sed -i "" -e /opie/s/^/#/ /etc/pam.d/*
```
- enlever le drapeau setuid du binaire opiepasswd. Pour cela :

```
chflags noschg /usr/bin/opiepasswd  
chmod 555 /usr/bin/opiepasswd  
chflags schg /usr/bin/opiepasswd
```

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité FreeBSD SA-06:12.opie du 22 mars 2006 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:12.opie.asc>
- Référence CVE CVE-2006-1283 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1283>

Gestion détaillée du document

23 mars 2006 version initiale.