

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur OpenSSH

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-152>

Gestion du document

Référence	CERTA-2003-AVI-152-002
Titre	Vulnérabilité du serveur OpenSSH
Date de la première version	17 septembre 2003
Date de la dernière version	1er octobre 2003
Source(s)	Avis de sécurité OpenSSH
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- Exécution distante de code arbitraire avec les privilèges du service *sshd* (généralement *root*).

2 Systèmes affectés

Tout système utilisant *OpenSSH* dans une version antérieure et incluant la 3.7.

3 Résumé

Des bogues ont été découverts dans le code du serveur *sshd* d'*OpenSSH*. Il induit un risque d'exécution de code arbitraire à distance.

4 Description

Une mauvaise gestion dans l'allocation mémoire des tampons peut générer un état incohérent qui pourrait être exploité pour réaliser un débordement de mémoire dans des conditions bien particulières. La revue du code consécutive a donné lieu à d'autres corrections sur la libération ou l'allocation des tampons.

5 Contournement provisoire

Restreindre à une liste de machines considérées comme sûres, les adresses IP autorisées à se connecter au serveur.

6 Solution

Mettre à jour *OpenSSH*.

- Code source (version 3.7.1p2 au moins) :
<http://www.openssh.com>
- Linux Red Hat :
<https://rhn.redhat.com/errata/RHSA-2003-279.html>
<https://rhn.redhat.com/errata/RHSA-2003-280.html>
- Mandrake Linux :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:090-1>
- Debian GNU/Linux :
<http://www.debian.org/security/2003/dsa-382>
<http://www.debian.org/security/2003/dsa-383>
- SuSE Linux :
http://www.suse.com/de/security/2003_039_openssh.html
- Slackware Linux :
<http://slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.372394>
- Sun Solaris :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56861>
- HP-UX :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0309-282>
- SGI Irix :
<ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc>
- Sun :
 - Solaris :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56861>
 - Linux et Cobalt :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56862>
- FreeBSD :
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:12.openssh.asc>
- NetBSD :
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-012.txt.asc>
- OpenBSD :
<http://openbsd.org/errata.html#sshbuffer>
- Cisco :
<http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml>
- Netscreen :
http://www.netscreen.com/services/security/alerts/openssh_1.jsp

7 Documentation

- Avis de sécurité OpenSSH :
<http://www.openssh.com/txt/buffer.adv>
- Référence CVE CAN-2003-0693 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0693>
- Référence CVE CAN-2003-0695 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0695>

- Référence CVE CAN-2003-0682 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0682>
- Avis du CERT/CC :
<http://www.cert.org/advisories/CA-2003-24.html>
<http://www.kb.cert.org/vuls/id/333628>

Gestion détaillée du document

17 septembre 2003 version initiale ;

24 septembre 2003 mise à jour des documents des vendeurs, ajouts de Sun, Cisco et Netscreen ;

1er octobre 2003 ajouts de HP, SGI, Sun.