



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 avril 2004
N° CERTA-2003-AVI-067-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les émulateurs de terminaux

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-067>

Gestion du document

Référence	CERTA-2003-AVI-067-002
Titre	Vulnérabilité dans les émulateurs de terminaux
Date de la première version	28 mars 2003
Date de la dernière version	29 avril 2004
Source(s)	Bulletin de Digital Defense Incorporated
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

- Injection de données ;
- exécution de commandes arbitraires.

2 Systèmes affectés

- aterm 0.4.x ;
- Eterm 0.9.x (Eterm 0.9.2 n'est pas vulnérable) ;
- gnome-terminal 2.x ;
- hanterm-xf 2.x ;
- Konsole 3.x ;
- putty 0.5x ;
- rxvt 2.7.x ;
- SecureCRT 3.x ;
- dtterm.

3 Résumé

Une vulnérabilité a été découverte dans plusieurs émulateurs de terminaux permettant à un individu mal intentionné de détourner des actions effectuées par l'utilisateur du terminal.

4 Description

Une séquence d'échappement est constitué d'une série de caractères débutant par un caractère d'échappement (0x1B) suivi d'une séquence de caractères ordinaires.

Une mauvaise gestion des séquences d'échappement dans plusieurs émulateurs de terminaux permet à un individu mal intentionné de tromper la vigilance d'un utilisateur afin d'exécuter des commandes arbitraires ou de modifier certains fichiers.

5 Solution

Appliquer les correctifs suivants les terminaux utilisés :

Vulnérabilité dans l'émulateur de terminaux `rxvt` :

- Bulletin de sécurité Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:034>
- Bulletin de sécurité RedHat :
<http://rhn.redhat.com/errata/RHSA-2003-054.html>
- Bulletin de sécurité Gentoo :
<http://forums.gentoo.org/viewtopic.php?t=42582>

Vulnérabilité dans l'émulateur de terminaux `gnome-terminal` :

- Bulletin de sécurité RedHat :
<http://rhn.redhat.com/errata/RHSA-2003-053.html>

Vulnérabilité dans l'émulateur de terminaux `Eterm` :

- Bulletin de sécurité Gentoo :
<http://www.securityfocus.com/advisories/5034>
- Bulletin de sécurité Debian DSA-496 :
<http://www.debian.org/security/2004/dsa-496>

Vulnérabilité dans l'émulateur de terminaux `dtterm` :

- Bulletin de sécurité HPSBUX0401-309 "SSRT3507 dtterm" de Hewlett-Packard :
<http://itrc.hp.com>

6 Documentation

- Bulletin Digital Defense Incorporated :
<http://digitaldefense.net/labs/papers/Termulation.txt>
- Emulateur de terminaux `rxvt` :
 - Référence CVE CAN-2003-0022 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0022>
 - Référence CVE CAN-2003-0023 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0023>
 - Référence CVE CAN-2003-0066 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0066>
- Emulateur de terminaux `gnome-terminal` :
 - Référence CVE CAN-2003-0070 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0070>
- Emulateur de terminaux `Eterm` :
 - Référence CVE CAN-2003-0021 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0021>

- Référence CVE CAN-2003-0068 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0068>
- Emulateur de terminaux `uxterm` :
 - Référence CVE CAN-2003-0065 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0065>
- Emulateur de terminaux `xterm` :
 - Référence CVE CAN-2003-0063 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0063>
 - Référence CVE CAN-2003-0071 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0071>
- Emulateur de terminaux `dtterm` :
 - Référence CVE CAN-2003-0064 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0064>
 - Référence CVE CAN-2003-0065 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0065>
- Emulateur de terminaux `putty` :
 - Référence CVE CAN-2003-0069 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0069>
- Emulateur de terminaux `hanterm-xf` :
 - Référence CVE CAN-2003-0078 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0078>
 - Référence CVE CAN-2003-0079 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0079>

Gestion détaillée du document

28 mars 2003 version initiale.

23 janvier 2004 Ajout référence au bulletin de sécurité HPSBUX0401-309 de Hewlett-Packard.

29 avril 2004 Ajout référence au bulletin de sécurité Debian.