

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans xterm

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-2009-AVI-002>

Gestion du document

Référence	CERTA-2009-AVI-002
Titre	Vulnérabilité dans xterm
Date de la première version	05 janvier 2009
Date de la dernière version	–
Source(s)	Rapport de bogue Debian 510030
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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de `xterm` antérieures à 238-1 sous Debian.

3 Résumé

Une vulnérabilité a été identifiée dans l'émulateur de terminal standard `xterm` sous Debian. Elle permet à une personne malveillante distante d'exécuter du code arbitraire sur le poste ayant une version vulnérable.

4 Description

Une vulnérabilité a été identifiée dans l'émulateur de terminal standard `xterm` sous Debian. L'interprétation de certains noms de commande n'est pas correctement effectuée dans une `DECRQSS` (*Device Control Request Status String*). Cela permettrait à une personne malveillante distante d'exécuter des commandes arbitraires.

Cette vulnérabilité est à mettre en relation avec des corrections apportées en 2003 et 2006 à l'application.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Rapport de bogue Debian 510030 du 28 décembre 2008 :
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=510030>
- Rapport de bogue Debian 384593 du 25 août 2006 :
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=384593>
- Référence CVE CVE-2003-0063 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0063>
- Référence CVE CVE-2003-0071 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0071>
- Référence CVE CVE-2006-7236 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7236>
- Référence CVE CVE-2008-2383 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2383>
- Avis CERTA-2003-AVI-067 du 28 mars 2003 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-067/>

Gestion détaillée du document

05 janvier 2009 version initiale.