

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans *xrdb* (X.Org)

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-2011-AVI-191>

Gestion du document

Référence	CERTA-2011-AVI-191
Titre	Vulnérabilité dans <i>xrdb</i> (X.Org)
Date de la première version	06 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité X.Org
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 ;
- élévation de privilèges.

2 Systèmes affectés

- *xrdb* versions 1.0.8 et inférieures ;
- X11R7.6 (*xrdb* 1.0.7 y est inclus).

3 Résumé

Une vulnérabilité permettant une exécution de code arbitraire à distance a été découverte dans *xrdb*.

4 Description

Une vulnérabilité a été découverte dans *xrdb*. Elle provient d'une mauvaise gestion des noms d'hôtes présents dans la base de ressources accédée via *xrdb* par certains gestionnaires d'affichage. Elle permet à une personne malintentionnée d'exécuter des commandes sous l'identité de l'utilisateur `root`. Ce type d'attaque n'est cependant

possible que si l'attaquant dispose d'un moyen de remplacer le nom d'hôte de la machine par un nom d'hôte spécialement forgé. Ainsi seules les machines définissant leur nom d'hôte via le protocole DHCP ou autorisant les connexions distantes via *xdmcp* sont vulnérables.

5 Solution

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

6 Documentation

- Référence CVE CVE-2011-0465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0465>
- Bulletin de sécurité X.Org :
<http://lists.freedesktop.org/archives/xorg-announce/2011-April/001636.html>

Gestion détaillée du document

06 avril 2011 version initiale.