

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Xerox FreeFlow Print Server

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-476>

Gestion du document

Référence	CERTA-2011-AVI-476
Titre	Vulnérabilités dans Xerox FreeFlow Print Server
Date de la première version	29 août 2011
Date de la dernière version	–
Source	Bulletin de sécurité Xerox XRX11-003 du 19 août 2011
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 ;
- exécution de code arbitraire ;
- déni de service à distance ;
- déni de service ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Xerox FreeFlow Print Server.

3 Résumé

De nombreuses vulnérabilités de Xerox FreeFlow Print Server ont été corrigées. Certaines permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Xerox FreeFlow Print Server utilise Solaris et Java, pour lesquels des vulnérabilités ont été corrigées. Certaines de ces vulnérabilités permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Xerox XRX11-003 du 19 août 2011 :
http://www.xerox.com/download/security/security-bulletin/127e996-10b83-4ab94539ab540/cert_XRX-003_v1.0.pdf
- Document du CERTA CERTA-2011-AVI-400 du 20 juillet 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-400/index.html>
- Référence CVE CVE-2011-0579 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0579>
- Référence CVE CVE-2011-0618 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0618>
- Référence CVE CVE-2011-0619 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0619>
- Référence CVE CVE-2011-0620 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0620>
- Référence CVE CVE-2011-0621 CVE-2011-0622 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0621 CVE-2011-0622>
- Référence CVE CVE-2011-0623 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0623>
- Référence CVE CVE-2011-0624 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0624>
- Référence CVE CVE-2011-0625 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0625>
- Référence CVE CVE-2011-0626 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0626>
- Référence CVE CVE-2011-0627 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0627>
- Référence CVE CVE-2011-0628 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0628>
- Référence CVE CVE-2011-1910 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1910>
- Référence CVE CVE-2011-2245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2245>
- Référence CVE CVE-2011-2249 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2249>
- Référence CVE CVE-2011-2258 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2258>
- Référence CVE CVE-2011-2259 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2259>
- Référence CVE CVE-2011-2285 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2285>
- Référence CVE CVE-2011-2287 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2287>

- Référence CVE CVE-2011-2289 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2289>
- Référence CVE CVE-2011-2290 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2290>
- Référence CVE CVE-2011-2291 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2291>
- Référence CVE CVE-2011-2294 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2294>
- Référence CVE CVE-2011-2295 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2295>
- Référence CVE CVE-2011-2298 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2298>

Gestion détaillée du document

29 août 2011 version initiale.