

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans Xen**

### Gestion du document

Référence	CERTFR-2015-AVI-458
Titre	Multiples vulnérabilités dans Xen
Date de la première version	30 octobre 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Xen XSA-152 du 30 octobre 2015 Bulletin de sécurité Xen XSA-151 du 30 octobre 2015 Bulletin de sécurité Xen XSA-150 du 30 octobre 2015 Bulletin de sécurité Xen XSA-149 du 30 octobre 2015 Bulletin de sécurité Xen XSA-148 du 30 octobre 2015 Bulletin de sécurité Xen XSA-147 du 30 octobre 2015 Bulletin de sécurité Xen XSA-146 du 30 octobre 2015 Bulletin de sécurité Xen XSA-145 du 30 octobre 2015
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(s)

- déni de service
- élévation de privilèges

### 2 - Systèmes affectés

- Xen versions 3.4.x et antérieures
- Xen versions 4.0 et postérieures
- Toutes les versions de Xen supportant ARM

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Xen*. Elles permettent à un attaquant de provoquer un déni de service et une élévation de privilèges.

## 4 - Solution

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

## 5 - Documentation

- Bulletin de sécurité Xen XSA-152 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-152.html>
- Bulletin de sécurité Xen XSA-151 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-151.html>
- Bulletin de sécurité Xen XSA-150 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-150.html>
- Bulletin de sécurité Xen XSA-149 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-149.html>
- Bulletin de sécurité Xen XSA-148 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-148.html>
- Bulletin de sécurité Xen XSA-147 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-147.html>
- Bulletin de sécurité Xen XSA-146 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-146.html>
- Bulletin de sécurité Xen XSA-145 du 30 octobre 2015  
<http://xenbits.xen.org/xsa/advisory-145.html>
- Référence CVE CVE-2015-7812  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7812>
- Référence CVE CVE-2015-7813  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7813>
- Référence CVE CVE-2015-7814  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7814>
- Référence CVE CVE-2015-7835  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7835>
- Référence CVE CVE-2015-7969  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7969>
- Référence CVE CVE-2015-7970  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7970>
- Référence CVE CVE-2015-7971  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7971>
- Référence CVE CVE-2015-7972  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7972>

## Gestion détaillée du document

**30 octobre 2015** version initiale.

---

Conditions d'utilisation de ce document :	<a href="http://cert.ssi.gouv.fr/cert-fr/apropos.html">http://cert.ssi.gouv.fr/cert-fr/apropos.html</a>
Dernière version de ce document :	<a href="http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-458">http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-458</a>

---