

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans glibc

Gestion du document

Référence	CERTFR-2016-AVI-066
Titre	Vulnérabilité dans glibc
Date de la première version	17 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-3481-1 du 16 février 2016 Bulletin de sécurité RedHat RHSA-2016:0175-1 du 16 février 2016 Bulletin de sécurité Suse SUSE-SU-2016:0471-1 du 16 février 2016 Bulletin de sécurité Ubuntu USN-2900-1 du 16 février 2016
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)

– exécution de code arbitraire à distance

2 - Systèmes affectés

Toutes les versions ultérieures à 2.9

3 - Résumé

Une vulnérabilité a été corrigée dans *glibc*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Debian DSA-3481-1 du 16 février 2016
<https://www.debian.org/security/2016/dsa-3481>
- Bulletin de sécurité RedHat RHSA-2016:0175-1 du 16 février 2016
<http://rhn.redhat.com/errata/RHSA-2016-0175.html>
- Bulletin de sécurité Suse SUSE-SU-2016:0471-1 du 16 février 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20160471-1.html>
- Bulletin de sécurité Ubuntu USN-2900-1 du 16 février 2016
<http://www.ubuntu.com/usn/usn-2900-1/>
- Référence CVE CVE-2015-7547
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547>

Gestion détaillée du document

17 février 2016 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-066>
