

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTFR-2016-AVI-099 |
| Titre | Multiples vulnérabilités dans le noyau Linux d'Ubuntu |
| Date de la première version | 15 mars 2016 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Ubuntu USN-2928-1 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2928-2 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2930-1 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2930-2 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2931-1 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2929-2 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2929-1 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2932-1 du 14 mars 2016 Bulletin de sécurité Ubuntu USN-2927-1 du 14 mars 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
- exécution de code arbitraire
- déni de service à distance
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Ubuntu 12.04 LTS
- Ubuntu 14.04 LTS
- Ubuntu 15.10

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux d'Ubuntu*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une exécution de code arbitraire et un déni de service 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 Ubuntu USN-2928-1 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2928-1/>
- Bulletin de sécurité Ubuntu USN-2928-2 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2928-2/>
- Bulletin de sécurité Ubuntu USN-2930-1 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2930-1/>
- Bulletin de sécurité Ubuntu USN-2930-2 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2930-2/>
- Bulletin de sécurité Ubuntu USN-2931-1 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2931-1/>
- Bulletin de sécurité Ubuntu USN-2929-2 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2929-2/>
- Bulletin de sécurité Ubuntu USN-2929-1 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2929-1/>
- Bulletin de sécurité Ubuntu USN-2932-1 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2932-1/>
- Bulletin de sécurité Ubuntu USN-2927-1 du 14 mars 2016
<http://www.ubuntu.com/usn/usn-2927-1/>
- Référence CVE CVE-2013-4312
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4312>
- Référence CVE CVE-2015-7566
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7566>
- Référence CVE CVE-2015-7833
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7833>
- Référence CVE CVE-2015-8767
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8767>
- Référence CVE CVE-2016-0723
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0723>
- Référence CVE CVE-2016-1977
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1977>
- Référence CVE CVE-2016-2069
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2069>
- Référence CVE CVE-2016-2384
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2384>
- Référence CVE CVE-2016-2543
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2543>
- Référence CVE CVE-2016-2544
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2544>
- Référence CVE CVE-2016-2545
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2545>
- Référence CVE CVE-2016-2546
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2546>

- Référence CVE CVE-2016-2547
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2547>
- Référence CVE CVE-2016-2548
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2548>
- Référence CVE CVE-2016-2549
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2549>
- Référence CVE CVE-2016-2782
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2782>
- Référence CVE CVE-2016-2790
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2790>
- Référence CVE CVE-2016-2791
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2791>
- Référence CVE CVE-2016-2792
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2792>
- Référence CVE CVE-2016-2793
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2793>
- Référence CVE CVE-2016-2794
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2794>
- Référence CVE CVE-2016-2795
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2795>
- Référence CVE CVE-2016-2796
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2796>
- Référence CVE CVE-2016-2797
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2797>
- Référence CVE CVE-2016-2798
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2798>
- Référence CVE CVE-2016-2799
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2799>
- Référence CVE CVE-2016-2800
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2800>
- Référence CVE CVE-2016-2801
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2801>
- Référence CVE CVE-2016-2802
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2802>
- Référence CVE CVE-2016-3134
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3134>
- Référence CVE CVE-2016-3135
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3135>

Gestion détaillée du document

15 mars 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-099>
