

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans VMware Workstation

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTFR-2017-AVI-074 |
| Titre | Multiples vulnérabilités dans VMware Workstation |
| Date de la première version | 10 mars 2017 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité VMware VMSA-2017-0003 du 09 mars 2017 |
| 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 à distance
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- VMware Workstation Pro versions antérieures à 12.5.3 sur Windows
- VMware Workstation Player versions antérieures à 12.5.3 sur Windows

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *VMware Workstation*. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données 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 VMware VMSA-2017-0003 du 09 mars 2017
<http://www.vmware.com/security/advisories/VMSA-2017-0003.html>
- Référence CVE CVE-2017-4898
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4898>
- Référence CVE CVE-2017-4899
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4899>
- Référence CVE CVE-2017-4900
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4900>

Gestion détaillée du document

10 mars 2017 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-2017-AVI-074>
