

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-026

1 - BMC (publication de code)

Dans son bulletin d'actualité du 25 avril 2016, l'ANSSI publiait un article sur l'utilisation de la zone tampon graphique du protocole RDP (cf. Documentation).

L'ANSSI a réalisé une implémentation en Python permettant d'obtenir des données exploitables depuis les fichiers Bitmap Cache. L'outil produit des images de 64x64 pixels au format BMP extraites des fichiers de la zone tampon. Il est désormais disponible sur son compte GitHub (cf. Documentation).

Documentation

- Implémentation de code (Python) :
<https://github.com/ANSSI-FR/bmc-tools/>
- Article de référence :
<http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-017/index.html>

2 - Rappel des avis émis

Dans la période du 20 au 26 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-215 : Multiples vulnérabilités dans WordPress
- CERTFR-2016-AVI-216 : Vulnérabilité dans Apple Airport
- CERTFR-2016-AVI-217 : Vulnérabilité dans Citrix XenMobile MDX Toolkit et Worx Home
- CERTFR-2016-AVI-218 : Vulnérabilité dans Trend Micro Deep Discovery Inspector

Gestion détaillée du document

27 juin 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-ACT-026>
