Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 12 juin 2017
N° CERTFR-2017-ACT-024

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-024

1 - EternalMiner : exploitation de la vulnérabilité SambaCry

Contexte

La CVE-2017-7494, plus communément appelée SambaCry en référence au rançongiciel WannaCry, est une vulnérabilité critique annoncée le 24 mai 2017 dans le logiciel Samba. Elle permet à un attaquant de prendre le contrôle à distance d'un système Linux.

Elle affecte toutes les versions de Samba à partir de la version 3.5.0 sortie le 1er Mars 2010, et est corrigée le 24 mai dans les versions 4.6.4/4.5.10/4.4.14.

Une campagne surnommée "EternalMiner" exploite actuellement cette vulnérabilité. D'après Kaspersky, elle aurait commencé le 30 mai, soit une semaine après son annonce.

Dans le cadre de cette campagne, les serveurs Samba vulnérables à SambaCry ouverts sur Internet sont exploités dans le but d'installer une porte dérobée sur le système ainsi qu'un logiciel mineur de crypto monnaie Monero.

Ce logiciel est une version modifiée de "CPUMiner", un projet source ouverte de minage de crypto monnaie.

A ce jour, l'exploitation de SambaCry dans le cadre de cette campagne mène au téléchargement de ces fichiers suivants :

- `INAebsGB.so`, une porte dérobée qui permet à l'attaquant d'accéder au système grâce à une connexion inversée;
- `cbIRWuoCc.so`, un exécutable contenant la charge utile pour récupérer le logiciel de minage de Monero.

Ce dernier effectue une commande bash qui récupère le mineur à l'aide de `wget` ou `curl` selon ce qui est installé sur la machine infectée, puis le lance en tâche de fond à l'aide de `nohup`. Néanmoins, au contraire de WannaCry, les versions actuelles d'EternalMiner ne tentent pas de se répliquer sur le réseau.

Recommandations

Le CERT-FR recommande l'application immédiate des mises à jour de sécurité permettant de corriger les failles exploitées dans le logiciel Samba, ainsi que de limiter l'exposition de Samba, en particulier sur Internet.

Documentation

- Avis CERT-FR CERTFR-2017-AVI-165
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-165/CERTFR-2017-AVI-165.html
- Bulletin de sécurité Samba du 23 mars 2017
  https://www.samba.org/samba/security/CVE-2017-2619.html

2 - Rappel des avis émis

Dans la période du 05 au 11 juin 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-167 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-168 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2017-AVI-169 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-170 : Multiples vulnérabilités dans VMware vSphere Data Protection (VDP)
- CERTFR-2017-AVI-171 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-172 : Vulnérabilité dans Citrix XenMobile Server

Gestion détaillée du document

12 juin 2017 version initiale.