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 13 mars 2017
N° CERTFR-2017-ACT-011

**Affaire suivie par :**
CERT-FR

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTFR-2017-ACT-011**

## 1 - Artéfact d'exécution lié à l'utilisation de l'outil SCCM

Lors du traitement d'un incident de sécurité ou d'une recherche de compromission, sur un simple poste ou sur un système d'information conséquent, les artéfacts d'exécution sont toujours une source d'information non négligeable pour déterminer si une application a été lancée sur un système.

Outre les artéfacts classiques d'exécution tels que les fichiers Prefetch, la base de registre (UserAssist, MUI Cache, AppcompatCache, ...) ou bien les journaux d'évènements, il est possible de s'appuyer sur des artéfacts plus spécifiques et souvent moins connus mais qui s'avèrent tout aussi utiles.

Dans le cas d'un parc important, il n'est pas rare que celui-ci dispose d'un serveur SCCM (System Center Configuration Manager) permettant une gestion centralisée et simplifiée du parc. SCCM permet, entre autres, d'effectuer des actions telles que la gestion de correctifs de sécurité, la télédistribution de logiciels, la prise en main à distance mais aussi l'inventaire matériel et logiciel du parc. Cette solution est éditée par Microsoft et repose sur une architecture client-serveur s'appuyant sur le service de gestion Windows Management Instrumentation (WMI).

Outre le fait que le serveur soit capable de fournir des informations utiles pour un analyste, il est intéressant de noter que le client stocke, et ce par défaut, des enregistrements CCM_RecentlyUsedApps au sein de la base CIM. Ces enregistrements correspondent à différentes informations concernant les fichiers exécutés allant du nom du fichier à son chemin mais aussi sa taille et sa date de dernière exécution. L'accès à ces informations s'effectue par l'intermédiaire de la classe CCM_RecentlyUsedApps de l'espace de nom root\ccm\SoftwareMeteringAgent. Les enregistrements CCM_RecentlyUsedApps disposent d'un entête facilement identifiable et il est donc possible d'extraire l'ensemble des enregistrements qu'ils soient alloués ou non.

Fireye a publié un outil en fin d'année dernière permettant de traiter cet artéfact en s'appuyant sur le contenu du fichier OBJECTS.DATA, qui correspond à la base CIM et contient les ressources relatives à WMI. Il se trouve par défaut au sein du répertoire SystemRoot\System32\wbem\Repository. Plus récemment, cet artéfact a été évoqué sur le blog 4n6ir avec la publication d'un script pour l'outil d'investigation EnCase.

D'une manière plus globale et pour compléter le bulletin d'actualité CERTFR-2016-ACT-029 lié à la collecte d'artéfacts dans le cadre de l'investigation numérique à grande échelle, il est utile de collecter le contenu du répertoire SystemRoot\System32\wbem\Repository. Outre le fait de pouvoir traiter l'artéfact lié à SCCM décrit ci-dessus, le contenu de ce répertoire est aussi utile pour l'investigation des aspects liés à la persistance WMI.

### Documentation

- https://www.fireeye.com/blog/threat-research/2016/12/do_you_see_what_icc.html
- http://blog.4n6ir.com/2017/02/secret-archives-of-execution-evidence
- http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ACT-029/index.html

# 2 - Cloudbleed : vulnérabilité dans Cloudflare

Cloudbleed est le nom donné à une vulnérabilité critique découverte dans Cloudflare par le chercheur Tavis Ormany de Google Project Zero. Elle a été découverte le 17 février, corrigée le lendemain, puis annoncée le 23 février sur le blog de l'éditeur. Cloudflare est utilisé pour la diffusion distribuée de contenus (CDN, ou *Content Delivery Network*), en particulier pour des raisons de protection contre les dénis de service. Son utilisation est largement répandue sur Internet : plusieurs millions de sites utilisent actuellement ce service, dont certains connus pour recevoir un trafic volumineux.

Cloudbleed est une vulnérabilité concernant une corruption mémoire qui permet à un attaquant de dévoiler des données résiduelles dans la mémoire des serveurs de Cloudflare, telles que des en-têtes HTTP, des jetons liés à l'authentification, des mots de passe ou des IPs de clients de Cloudflare. Le nom de cette vulnérabilité fait référence à Heartbleed, une vulnérabilité rendue publique le 7 avril 2014, dont l'impact ressemble à celui de Cloudbleed.

L'origine de cette vulnérabilité provient d'une erreur introduite le 22 septembre 2016 dans le code de l'analyseur syntaxique HTML utilisé par les fonctionnalités d'offuscation d'adresse mail, d'exclusion côté serveur et de réécriture automatique de liens HTTPS proposées par Cloudflare.

Deux conditions devaient être réunies afin de déclencher cette vulnérabilité :

- Un ensemble particulier de fonctionnalités de Cloudflare devaient être activées pour la page vulnérable;
- Le code HTML de la page en question devait être malformé d'une manière particulière.

Plus précisement, le code HTML devait se finir par un attribut de balise incorrectement fermé, par exemple une balise IMG dont l'attribut SRC n'est pas correctement fermé :

```
<IMG HEIGHT="50px" WIDTH="200px" SRC="
```

Lors de l'analyse syntaxique du code HTML, la présence de cet attribut malformé provoque un dépassement de tampon ayant pour effet d'interpréter le contenu à la suite du tampon comme du code HTML. Puisque l'attribut malformé est placé en fin de la page HTML, le contenu de la mémoire placé à la suite du tampon, quelque soit sa nature, est analysé à la place puis inclus dans la page HTML générée.

Le 13 février, alors que Cloudflare n'avait pas encore connaissance de l'existence de cette vulnérabilité, les circonstances permettant d'appeler le code erroné ont été élargies.

Par conséquent, Cloudflare a déclaré avoir relevé dans leurs journaux 605 037 occurrences de ce bug entre le 22 septembre 2016 et le 13 février 2017, puis 637 034 occurrences entre le 13 février et le 18 février au moment de la correction de la vulnérabilité, pour un total de 1 242 071 occurrences.

À noter que l'exploitation de cette vulnérabilité ne concerne pas seulement le site hébergeant la page vulnérable : l'exploitation de la page HTML malformée permet de récupérer de la mémoire provenant potentiellement d'autres sites utilisant les services de Cloudflare. Ainsi, selon l'agencement de la mémoire au moment de l'exploitation de la vulnérabilité, les informations d'autres sites pouvaient être divulguées.

## Recommandations

Le CERT-FR recommande aux utilisateurs des sites utilisant Cloudflare de changer les mots de passe utilisés pour les sites concernés. Pour rappel, l'ANSSI a publié sur son site des recommandations sur la sécurité des mots de passe.

### Documentation

- Recommandations de sécurité relatives aux mots de passe :
  https://www.ssi.gouv.fr/guide/mot-de-passe/
- Chaîne de mails de Google Project Zero concernant cette vulnérabilité :
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1139
- Annonces de Cloudflare concernant cette vulnérabilité :
  https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/
  https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed/

# 3 - Rappel des avis émis

Dans la période du 06 au 12 mars 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-ALE-004 : Vulnérabilité dans Apache Struts
- CERTFR-2017-AVI-065 : Multiples vulnérabilités dans Wireshark
- CERTFR-2017-AVI-066 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-067 : Multiples vulnérabilités dans WordPress
- CERTFR-2017-AVI-068 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTFR-2017-AVI-069 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2017-AVI-070 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-071 : Vulnérabilité dans Apache Struts
- CERTFR-2017-AVI-072 : Vulnérabilité dans SPIP
- CERTFR-2017-AVI-073 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2017-AVI-074 : Multiples vulnérabilités dans VMware Workstation

# Gestion détaillée du document

**13 mars 2017** version initiale.