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 07 mars 2016
N° CERTFR-2016-ACT-010

**Affaire suivie par :**
CERT-FR

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTFR-2016-ACT-010**

## Obsolescence des systèmes de gestion de contenu

Un site Internet constitue souvent la vitrine d'une entreprise, d'une collectivité locale ou d'une administration. Il peut également être une source de revenus (vente en ligne) ou un moyen d'accès à un réseau partenaire (scénario extranet). Sa disponibilité et son intégrité sont donc des besoins majeurs qu'il faut garantir.

Pour cela, les bonnes pratiques incluent, entre autres, l'utilisation de mots de passe complexes, une exposition limitée à Internet et la mise en place des correctifs de sécurité. A ce titre, les différentes briques qui composent le site doivent être maintenues à jour : le système d'exploitation, le service HTTP et le système de gestion de contenu (ou CMS). Il faut vérifier la disponibilité de correctifs auprès des éditeurs de ces différents composants. La démarche nécessite de mettre en place une veille active pour être notifié des futures publications.

Les conséquences possibles de l'exploitation d'une faille dans un système de gestion de contenu sont multiples. Il peut s'agir d'une défiguration, pouvant facilement porter atteinte à l'image de l'entreprise ou de la collectivité. Mais également l'insertion de code malveillant (qui sera potentiellement transmis à toute personne qui se connectera sur le site), l'utilisation du site à des fins malveillantes (diffusion de spam, hameçonnage, attaques en déni de service distribuées, relais de contrôle commande pour des maliciels, ...) ou l'exfiltration de données sensibles (informations personnelles, contrats engagés, etc.).

Pour mémoire, le début de l'année 2015 a été marqué par de nombreuses défigurations, qui ne sont qu'un exemple des conséquences possibles de l'absence de maintien à jour des sites internet. En effet, des attaquants peuvent facilement scanner des sites Internet de manière automatisée et massive à la recherche d'un système de gestion de contenu vulnérable.

Le CERT-FR attire votre attention sur le fait que de nombreuses attaques sur les sites Internet aboutissent en exploitant des vulnérabilités connues et corrigées des applications web en place. Les liens vers les dernières versions des systèmes de gestion de contenu les plus courants sont donnés en documentation.

### Documentation

- WordPress
  https://codex.wordpress.org/WordPress_Versions
- Joomla
  https://docs.joomla.org/What_version_of_Joomla!_should_you_use
- Drupal
  https://www.drupal.org/security
- Common Vulnerabilities and Exposures
  http://cve.mitre.org/
- Guides et recommandations de l'ANSSI :
  http://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-des-sites-web
  http://www.ssi.gouv.fr/actualite/proteger-son-site-internet-des-cyberattaques/

# 1 - Vulnérabilités OpenSSL DROWN et CacheBleed

Le 1er mars 2016, le CERT-FR a publié l'avis CERTFR-2016-AVI-076 concernant plusieurs vulnérabilités dans la bibliothèque cryptographique OpenSSL. 10 vulnérabilités ont été corrigées, dont 2 relatives à l'attaque nommée "DROWN" ont une gravité jugée élevée. Elles sont identifiées par les numéros CVE-2016-0703 et CVE-2016-0800. Une autre vulnérabilité, identifiée par la CVE-2016-0702, est une attaque temporelle et a été baptisée "CacheBleed".

## DROWN (CVE-2016-0800)

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) est une vulnérabilité qui affecte les serveurs supportant l'ancienne norme SSLv2 et utilisant le même certificat (donc la même clé privée de chiffrement) pour SSLv2 et TLS. De plus, l'échange des clés doit se faire via le protocole "RSA key exchange". L'exploitation de la vulnérabilité nécessite que l'attaquant soit présent sur le réseau, de manière passive dans un premier temps, puis de manière active dans un second temps. Le scénario d'attaque est le suivant:

L'attaquant doit écouter sur le réseau plusieurs centaines de connexions entre la victime et le serveur, peu importe le protocole utilisé (TLS ou SSL) afin de capturer les clés de session chiffrées qui transitent.

L'attaquant utilise ensuite une faiblesse connue de l'algorithme RSA, la "malléabilité", en envoyant au même serveur, des messages spécialement conçus à partir des données récupérées (via le protocole SSLv2 cette fois).

En fonction de la réponse du serveur, l'attaquant peut savoir si les modifications induites correspondent à un message valide. Si c'est le cas, l'attaquant est capable de remonter à la clé de session utilisée lors de la connexion et de déchiffrer le trafic correspondant à cette session uniquement. L'attaquant n'a pas accès à la clé privée de chiffrement du serveur, il ne pourra donc pas déchiffrer toutes les connexions.

## CacheBleed (CVE-2016-0702)

CacheBleed est une attaque par canaux auxiliaires qui exploite une fuite d'information du cache dans certains processeurs Intel. En surveillant les temps d'accès au cache, il est possible de retrouver des informations concernant les clés privées de chiffrement.

Bien qu'aujourd'hui les implémentations des algorithmes cryptographiques sont conçues pour être résistantes à ce type d'attaque, l'article associé à cette vulnérabilité démontre qu'il est effectivement possible de récupérer des clés RSA de taille 2048 ou 4096 bits. Néanmoins, étant donné que cette attaque nécessite un accès local à la machine pour exécuter le code, sa gravité est jugée faible.

### Détails de la vulnérabilité

Le cache du processeur est un espace mémoire qui permet de stocker certaines données afin d'y accéder plus rapidement. Il est ainsi possible de savoir si une donnée est déjà en cache, en analysant le temps mis pour la récupérer. Plus précisément, les lignes du cache sont divisées en bancs, qui contiennent chacun un nombre fixé d'octets.

Sur certains processeurs, le cache permet d'accéder simultanément à plusieurs bancs sur une même ligne mais il ne permet pas d'accéder simultanément au même banc.

Lorsque ceci se produit, un conflit de type "cache-banc" est généré et l'une des requêtes accède aux données, alors que les autres doivent attendre. Ce phénomène permet de retrouver l'exposant privé qui est utilisé lors de l'exponentiation modulaire réalisée par l'algorithme RSA. La clé privée de chiffrement peut ensuite être directement déduite de la connaissance de cet exposant.

## Recommandations

Le CERT-FR recommande d'installer ces mises à jour dès que possible.

### Documentation

- Site de la vulnérabilité DROWN
  https://drownattack.com
- Site de la vulnérabilité CacheBleed
  https://ssrg.nicta.com.au/projects/TS/cachebleed/

## 2 - Rappel des avis émis

Dans la période du 29 février au 06 mars 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-074 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-075 : Multiples vulnérabilités dans Ruby On Rails
- CERTFR-2016-AVI-076 : Multiples vulnérabilités dans OpenSSL
- CERTFR-2016-AVI-077 : Multiples vulnérabilités dans phpMyAdmin
- CERTFR-2016-AVI-078 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-079 : Vulnérabilité dans les commutateurs Cisco Nexus séries 3000 et 3500
- CERTFR-2016-AVI-080 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-081 : Multiples vulnérabilités dans SCADA les produits Schneider

## Gestion détaillée du document

**07 mars 2016** version initiale.