Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 29 novembre 2013
N° CERTA-2013-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-048

1 Découverte d'un ver ciblant les serveurs Apache Tomcat

Le 22 novembre 2013, Symantec a publié un article sur la découverte d'un nouveau ver se propageant via Apache Tomcat. L'infection s'effectue via l'utilisation des identifiants et mots de passe configurés par défaut sur les serveurs et possédant une interface d'administration accessible publiquement.

D'après Symantec, en plus de la réplication le ver installe, dans la plupart des cas observés, des codes PHP permettant la formation de botnets IRC, donnant par la suite aux « administrateurs » de ces botnets la possibilité d'effectuer des actions malveillantes sur les serveurs infectés ou de réaliser des attaques de type DDoS. D'après les analyses de Symantec, le ver n'aurait pas encore infecté de serveurs basés en France. Cependant, ce type de menace peut se répandre rapidement.

Le CERTA recommande donc de ne pas laisser l'interface d'administration des serveurs Tomcat accessibles publiquement et de procéder à la configuration d'un mot de passe robuste.

Plus généralement, le CERTA rappelle que toutes les interfaces d'administration doivent être accessibles, au niveau réseau, uniquement par les postes clairement définis. L'accès depuis les autres machines du réseau interne ou à partir d'Internet doit être prohibé. Ce cloisonnement peut être mis en place via une configuration adéquate des règles de pare-feu. Il est recommandé d'utiliser un réseau séparé physiquement ou logiquement pour les opérations d'administration (cf. Règle 29 du Guide d'hygiène informatique). Le changement des mots de passe par défaut des interfaces ainsi que leur renouvellement régulier est également indispensable conformément au document de « Recommandations de sécurité relatives aux mots de passe » publié sur le site de l'ANSSI.

Documentation

- Article Symantec :
  http://www.symantec.com/connect/blogs/all-your-tomcat-are-belong-bad-guys
- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe :
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

2 Utilisation de protocoles d'échanges de clés dotés de la propriété PFS

Récemment, Twitter a annoncé la généralisation de l'utilisation de protocoles d'échanges de clés dotés de la propriété cryptographique *Perfect Forward Secrecy* (PFS) pour conserver la confidentialité des échanges passés même en cas de compromission d'une clé privée de ses serveurs. Cette annonce est l'occasion pour le CERTA de rappeler l'intérêt de la mise en place d'une telle protection.

Le protocole TLS, largement répandu sur Internet, permet de sécuriser les échanges entre un client et un serveur en garantissant l'authentification du serveur (et selon les cas d'utilisation, celle du client), la confidentialité

et l'intégrité des données échangées. Le serveur distant dispose d'un couple clé publique / clé privée qui lui permet d'une part de s'authentifier auprès du client et d'autre part de sécuriser l'échange d'un secret partagé (appelé clé de session) utilisé pour chiffrer les échanges ultérieurs à la négociation.

Si une communication est interceptée, la compromission de la clé privée peut permettre, selon les protocoles d'échanges de clés utilisés, de récupérer la clé de session ayant servi à chiffrer la communication et donc de déchiffrer l'ensemble des données transmises à la suite de la négociation de cette clé de session.

La PFS est une propriété cryptographique permettant de garantir que la compromission d'une clé privée à un instant donné ne permet pas de déchiffer les clés de session protégées par cette clé privée et ne permet donc pas de déchiffrer les échanges précédents.

Cette propriété consiste alors à limiter l'usage de la clé privée du serveur à la phase d'authentification et faire en sorte que la négociation de la clé de session ne fasse pas intervenir la clé privée. La clé de session négociée est alors valable pendant une durée déterminée (durée de la connexion ou imposition de regénération de clé à intervalle régulier).

En pratique, cela se traduit par l'utilisation du protocole d'échange de clés *Diffie-Hellman* ou de sa variante utilisant les courbes elliptiques pour l'établissement de la clé de session.

Le CERTA recommande d'activer et de privilégier la PFS sur les serveurs web, dès lors que les équipements le permettent, par l'utilisation du protocole *Diffie-Hellman* éphémère classique ou sa variante sur courbes elliptiques qui présente de meilleures performances.

Le CERTA recommande également de forcer le renouvellement périodique des clés privées afin de limiter l'impact d'une compromission d'une telle clé sur le trafic des données.

Pour mémoire, l'ANSSI a publié sur son site des recommandations de sécurité relatives à IPsec pour la protection des flux réseau décrivant notamment la PFS.

Documentation

- Annonce de Twitter :
  https://blog.twitter.com/2013/forward-secrecy-at-twitter-0
- Recommandations de sécurité relatives à IPsec pour la protection des flux réseau :
  http://www.ssi.gouv.fr/ipsec
- SSL/TLS : état des lieux et recommandations :
  http://www.ssi.gouv.fr/IMG/pdf/SSL_TLS_etat_des_lieux_et_recommandations.pdf

3 Vulnérabilité dans l'interpréteur Ruby

La semaine dernière, un bulletin de sécurité concernant une vulnérabilité (CVE-2013-4164) au niveau de la gestion des nombres à virgule flottante dans Ruby a été publié.

3.1 Présentation de la vulnérabilité

Cette vulnérabilité de type « débordement dans le tas » affecte potentiellement toutes les applications utilisant l'interpréteur Ruby pour convertir des données provenant d'une source inconnue en nombres à virgule flottante.

L'exploitation de la vulnérabilité permet de causer un déni de service et potentiellement une exécution de code arbitraire.

L'expression suivante permet de tester la présence de la vulnérabilité (arrêt inopiné) :

```
$ ruby -e '("1." + "1"*400000).to_f'
```

Pour corriger cette vulnérabilité, le CERTA recommande d'installer la dernière mise à jour de Ruby. Le CERTA recommande également d'effectuer un inventaire des applications développées en Ruby, notamment les applications Ruby On Rails, et de vérifier si ces dernières sont impactées par cette vulnérabilité.

Il est à noter que la version 1.8 de Ruby est considérée comme obsolète et ne bénéficiera donc pas d'un correctif officiel pour cette vulnérabilité. Il est donc recommandé de migrer vers la branche 1.9 ou 2.0 qui sont supportées en matière de sécurité.

3.2 Versions affectées

- Toutes les versions de Ruby 1.8 ;
- Versions antérieures à Ruby 1.9.3-p484 ;
- Versions antérieures à Ruby 2.0.0-p353 ;
- Versions antérieures à Ruby 2.1.0 preview2 ;
- Versions antérieures à la révision 43780.

Documentation

- Bulletin de sécurité Ruby du 22 novembre 2013 :
  https://www.ruby-lang.org/en/news/2013/11/22/heap-overflow-in-floating-point-parsing-cve-2013-4164/
- Avis CERTA-2013-AVI-647 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-647/

4 Bonnes pratiques au téléphone (ou les combines du combiné)

Le CERTA a de temps à autre connaissance du fait qu'une personne prétendant agir en son nom est entrée en contact avec un organisme à propos d'un éventuel problème de sécurité informatique. Ce type d'appel, a priori anodin, peut être une manière, pour une personne malveillante, d'obtenir des informations sur une entreprise et son système d'information.

En cas de doute sur l'identité d'un appelant et son appartenance au CERTA, il est recommandé de ne pas hésiter à se faire préciser son nom, sa fonction ainsi que l'entité au nom de laquelle il s'exprime. Si le doute persiste, il est conseillé de rappeler l'interlocuteur du CERTA afin de s'assurer de la véracité de son identité.

Les coordonnées du CERTA sont disponibles sur son site Internet. Le CERTA est joignable :

- par téléphone au 01 71 75 84 50 de 08h30 à 18h30 du lundi au vendredi ;
- par téléphone au 01 71 75 84 68 en dehors des heures ouvrables ;
- par courriel adressé à certa-svp@certa.ssi.gouv.fr.

Documentation

- Page de contact du site du CERTA :
  http://www.certa.ssi.gouv.fr/certa/contact.html

5 Rappel des avis émis

Dans la période du 22 au 28 novembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-008 : Vulnérabilité critique dans le noyau de Microsoft Windows
- CERTA-2013-AVI-646 : Vulnérabilité dans Xen
- CERTA-2013-AVI-647 : Vulnérabilité dans Ruby
- CERTA-2013-AVI-648 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-649 : Multiples vulnérabilités dans les systèmes SCADA ABB
- CERTA-2013-AVI-650 : Multiples vulnérabilités dans Fujitsu Interstage HTTP Server

Gestion détaillée du document

29 novembre 2013 version initiale.