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 août 2017
N° CERTFR-2017-ACT-031

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-031

1 - Nouvelle vulnérabilité dans Apache Struts 2

Apache Struts est un cadriciel (*framework*) disponible en source ouverte et qui permet de développer des applications Web avec le langage Java (J2EE).

Depuis mars dernier, la vulnérabilité CVE-2017-5638 a été massivement exploitée pour déclencher des exécutions de code arbitraire à distance (cf. section Documentation). Celle-ci était introduite par un mauvais traitement de l'analyseur (*parser*) Multipart "Jakarta", lors d'un transfert de fichier depuis un client vers le serveur Web sur lequel est utilisé Apache Struts 2.

Le 7 juillet 2017, la fondation Apache a publié l'alerte de sécurité S2-048 (cf. section Documentation). La vulnérabilité CVE-2017-9791 permet également une exécution de code arbitraire mais son impact est moins important que la vulnérabilité CVE-2017-5638.

D'abord, parce que seules les versions 2.3.x sont vulnérables ; ensuite car la vulnérabilité impacte le greffon Struts 1. Celui-ci sert à importer les classes Struts 1 *Actions* et *ActionsForms* dans des applications Struts 2.

Si ce greffon est présent par défaut, il faut en revanche que la classe *ActionMessage*, contenant la vulnérabilité, soit instanciée pour que l'application soit vulnérable.

Plus concrètement, Apache recommande de ne jamais passer des données fournies par l'utilisateur directement au constructeur de la classe ActionMessage. Les appels au constructeur doivent donc être de cette forme :

```
messages.add("msg", new ActionMessage("struts1.gansterAdded", gform.getName()));
```

Et non pas :

```
messages.add("msg", new ActionMessage("Ganster " + gform.getName() + "was added");
```

En effet, dans le second cas, si les données utilisateurs prennent la forme d'une expression *Object Graph Navigation Language (OGNL)* valide, celles-ci seront interprétées par le serveur comme du code à exécuter. A noter que plusieurs preuves de concept sont disponibles publiquement sur internet.

Lorsque l'on installe Struts, plusieurs formulaires sont fournis à titre d'exemples. Afin de pouvoir les tester, les archives *.war* doivent être copiées dans l'arborescence du serveur. Ces applications de test ne doivent en aucun cas se retrouver en environnement de production. A plus forte raison ici car l'une d'entre elles est vulnérable. Le formulaire *Gangster.action*, contenu dans l'archive *struts2-showcase.war*, utilise le code fourni ci-dessus à titre de contre-exemple.

Pour vérifier si son serveur est vulnérable, il suffit de tester l'URI suivante:

```
/struts2-showcase/integration/
```

Si la réponse est positive, il faut au plus vite supprimer le répertoire *struts2-showcase* ainsi que l'archive *.war* correspondante de l'arborescence de son serveur.

Bien que moins critique que la vulnérabilité CVE-2017-5638, cette nouvelle vulnérabilité dans Struts sert à illustrer deux principes de base :

– Les soins à porter à la configuration de ses services.

– Le besoin de filtrer les données utilisateurs correctement.

Documentation

– Bulletin d'alerte du CERT-FR (CERTFR-2017-ALE-004) :
http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-004/index.html
– Bulletin de sécurité Apache (S2-048) :
https://cwiki.apache.org/confluence/display/WW/S2-048
– Référence CVE (CVE-2017-9791) :
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9791
– Billet Trend Micro :
http://blog.trendmicro.com/trendlabs-security-intelligence/examining-cve-2017-9791-new-apache-struts-remote-code-execution-vulnerability/
– Billet McAfee :
https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-cve-2017-9791-apache-struts-vulnerability-can-lead-remote-code-execution/

2 - Rappel des avis émis

Dans la période du 31 juillet au 06 août 2017, le CERT-FR a émis les publications suivantes :

– CERTFR-2017-AVI-242 : Multiples vulnérabilités dans FreeRDP
– CERTFR-2017-AVI-243 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2017-AVI-244 : Vulnérabilité dans Google Chrome OS
– CERTFR-2017-AVI-245 : Vulnérabilité dans le noyau Linux de RedHat
– CERTFR-2017-AVI-246 : Multiples vulnérabilités dans PHP
– CERTFR-2017-AVI-247 : Multiples vulnérabilités dans le noyau Linux d' Ubuntu

Durant la même période, les publications suivantes ont été mises à jour :
– CERTFR-2017-ALE-012 : Campagne de maliciels prenant l'apparence d'un rançongiciel à multiples capacités de propagation (clôture de l'alerte ;)
– CERTFR-2017-AVI-233 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu (ajout du bulletin de sécurité Ubuntu USN-3371-1 du 28 juillet 2017.)

Gestion détaillée du document

07 août 2017 version initiale.