Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juillet 2013
N° CERTA-2013-ACT-029

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-029

1 Deux nouvelles vulnérabilités liées à OGNL dans Apache Struts 2

Le projet Apache Struts 2 a publié très récemment deux bulletins de sécurité S2-016 et S2-017 concernant des vulnérabilités liées à OGNL, langage permettant d'accéder aux attributs d'objets Java et d'appeler certaines méthodes de classe.

Depuis 2010, ce cadriciel, fréquemment utilisé pour le développement d'applications Web, a fait l'objet d'un certain nombre de bulletins de sécurité concernant cette fonctionnalité. Ces vulnérabilités, relativement simples à exploiter, permettent souvent d'exécuter à distance du code arbitraire au niveau du serveur qui héberge l'application.

La première vulnérabilité relevée par le bulletin S2-016 (CVE-2013-2251) concerne des fonctionnalités de redirection fournies par ce cadriciel. Celles-ci permettent, par exemple, d'ajouter des informations de navigation aux boutons des formulaires définis dans les modèles.

Lors de la réception de la requête HTTP envoyée par le client, ces informations sont ensuite évaluées en tant qu'expressions OGNL par le cadriciel. La vulnérabilité est liée au fait que ces chaînes de caractères, possiblement injectées depuis le navigateur d'un attaquant, ne sont pas contrôlées avant leur évaluation. Ceci peut ainsi mener à une exécution de code arbitraire, liées aux fonctionnalités offertes par OGNL, à savoir :

- l'accès à des variables du contexte serveur ;
- la fuite d'informations pouvant faciliter une exploitation plus ciblée ;
- l'exécution de commandes pouvant endommager le fonctionnement de l'application.

Cette vulnérabilité est donc particulièrement critique car son exploitation peut aboutir à la compromission d'un serveur Web.

La deuxième vulnérabilité, décrite dans le bulletin S2-017 (CVE-2013-2248), est liée elle aussi aux deux préfixes *redirect:* et *redirectionAction:*. Leurs paramètres peuvent être facilement manipulés pour effectuer des redirections vers une adresse arbitraire. La criticité de cette vulnérabilité est cependant moins importante.

Toute application utilisant Struts 2 est potentiellement vulnérable à l'exploitation d'une faille du cadriciel. Ces nouvelles vulnérabilités dans Struts 2 concernent l'ensemble des versions du cadriciel comprises entre 2.0.0 et 2.3.15.

Les cadriciels tels que Struts 2 sont utilisés dans une grande majorité d'applications mais ils sont rarement pris en compte dans les processus de maintien en condition de sécurité. Pourtant, en raison du nombre important de vulnérabilités publiées sur ces cadriciels, ces derniers constituent une cible de choix pour les attaquants. Le suivi des mises à jour de ces cadriciels est donc essentiel.

Il est à noter que ces mises à jour peuvent impacter le fonctionnement des applications en supprimant ou modifiant certaines fonctionnalités. Il est donc recommandé de se reporter aux indications des bulletins de sécurité et d'effectuer une revue manuelle du code afin de remplacer le code non-compatible.

Documentation

- Langage OGNL :
  http://commons.apache.org/proper/commons-ognl/
- Bulletin S2-016 :
  http://struts.apache.org/release/2.3.x/docs/s2-016.html
- Bulletin S2-017 :
  http://struts.apache.org/release/2.3.x/docs/s2-017.html

2 Périphériques USB promotionnels et cadeaux électroniques

Les clés USB publicitaires personnalisées sont régulièrement distribuées lors de salons ou conférences. Ces dernières peuvent constituer un vecteur d'attaque. En plus des piégeages classiques de type « autorun », elles peuvent contenir des fichiers malveillants ou exploiter des vulnérabilités spécifiques (cf vulnérabilité MS13-027).

Des piégeages matériels ne sont également pas à exclure. Des supports ainsi modifiés peuvent, par exemple, avoir des comportements différents lors du branchement du périphérique afin de cibler un utilisateur ou encore dissimuler des éléments pendant l'analyse du support ou le passage dans une « station blanche ».

En cas de doute sur un périphérique tel qu'une clé USB, il est recommandé de ne pas l'utiliser. La tentation est cependant plus grande lorsqu'il s'agit d'un téléphone ou d'une tablette ayant une valeur marchande plus importante. Les possibilités de compromission seront pourtant plus nombreuses et potentiellement plus complexes à analyser. Il sera alors très difficile de certifier l'intégrité de l'objet.

En dépit de la valeur du cadeau électronique, le CERTA recommande de ne pas utiliser en environnement professionnel des périphériques dont la provenance peut susciter un doute auprès de l'utilisateur. Dans le cas où une suspicion est décelée, il est également nécessaire de faire remonter cette information à l'officier de sécurité ou toute autre autorité compétente.

3 Mise à jour Oracle

Le 16 juillet 2013, Oracle a publié des mises à jour corrigeant de nombreuses vulnérabilités dans certains de ses produits tels que PeopleSoft, MySQL, Oracle Database, Solaris, etc.

Les vulnérabilités les plus critiques permettent l'exécution de code arbitraire à distance ou la divulgation de données confidentielles par un attaquant.

De nombreuses solutions tiers utilisent des composants Oracle. Des mises à jour de ces solutions sont donc à prévoir.

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Bulletin de sécurité Oracle CPUJuly2013 du 16 juillet 2013 :
  http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
- Bulletin de sécurité Oracle sur les produits tiers du 16 juillet 2013 :
  http://www.oracle.com/technetwork/topics/security/thirdparty-patch-map-1482893.html

4 Rappel des avis émis

Dans la période du 12 au 18 juillet 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-410 : Vulnérabilité dans Squid
- CERTA-2013-AVI-411 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTA-2013-AVI-412 : Multiples vulnérabilités dans le noyau Linux de Mandriva

- CERTA-2013-AVI-413 : Multiples vulnérabilités dans Juniper Junos
- CERTA-2013-AVI-414 : Vulnérabilité dans PHP
- CERTA-2013-AVI-415 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-416 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-417 : Multiples vulnérabilités dans Oracle Virtualization
- CERTA-2013-AVI-418 : Vulnérabilité dans Oracle iLearning
- CERTA-2013-AVI-419 : Multiples vulnérabilités dans Oracle MySQL
- CERTA-2013-AVI-420 : Vulnérabilité dans Oracle Industry Applications
- CERTA-2013-AVI-421 : Multiples vulnérabilités dans Oracle Database Server
- CERTA-2013-AVI-422 : Vulnérabilité dans Oracle Hyperion
- CERTA-2013-AVI-423 : Multiples vulnérabilités dans Oracle E-Business Suite
- CERTA-2013-AVI-424 : Multiples vulnérabilités dans Oracle Enterprise Manager Grid Control
- CERTA-2013-AVI-425 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTA-2013-AVI-426 : Multiples vulnérabilités dans Oracle PeopleSoft
- CERTA-2013-AVI-427 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite
- CERTA-2013-AVI-428 : Multiples vulnérabilités dans Oracle Supply Chain Products Suite
- CERTA-2013-AVI-429 : Vulnérabilité dans phpMyAdmin
- CERTA-2013-AVI-430 : Vulnérabilité dans Apache Struts
- CERTA-2013-AVI-431 : Multiples vulnérabilités dans Cisco Intrusion Prevention System
- CERTA-2013-AVI-432 : Multiples vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2013-AVI-433 : Multiples vulnérabilités dans EMC Avamar

Gestion détaillée du document

19 juillet 2013 version initiale.