Problema amb l'autentificació d'usuaris en Aplicacions Desenvolupades amb Canigó

Avis de Seguretat	
Versions de Canigó Afectades	**Totes (1.x i 2.x)**
Data publicació	**30/03/2009**
Descripció breu	**Bug a la llibreria Acegi permet saltar el sistema de securització per url**
Gravetat	**Alta**

Contingut

A qui va dirigit

Als responsables del desenvolupament d'aplicacions basades en Canigó i als responsables de les aplicacions ja desenvolupades i desplegades en els entorns d'Integració, Preproducció i Producció.

Versió de Canigó

El problema descrit en aquest document i la seva solució afecten a totes les versions de openFrame 1.x i Canigo 2.x

Introducció

S'ha detectat un problema en el funcionament d'Acegi, que és un dels components utilitzat internament pel Servei de Seguretat de Canigó.

Degut a aquest problema i en funció de la configuració que s'hagi fet del servei de seguretat

- és possible accedir a una aplicació sense necessitat d'un codi d'usuari i clau d'accés
- és possible, per un usuari d'una aplicació, accedir a les parts de l'aplicació que li haurien d'estar prohibides

El problema afecta tant a les aplicacions desenvolupades amb Canigó amb versió igual o superior a 2.2 (que utilitzen Acegi 0.9.0) com les desenvolupades amb Canigó 1.x o Canigó 2.x amb versió inferior 2.2 (que utilitzen Acegi 0.8.3).

Es proposa una solució consistent en la substitució de la llibreria d'Acegi que conté el problema per una llibreria en què s'ha incorporat la correcció.

Problema amb l'autentificació d'usuaris en Aplicacions Desenvolupades amb Canigó

Descripció del problema

En la configuració del servei de seguretat de Canigó (normalment en l'arxiu `canigo-services-security.xml` / `openframe-services-security.xml`) s'especifiquen les URLs de l'aplicació que queden protegides i els Rols que hi tenen accés.

Canigó utilitza la llibreria d'Acegi per validar que l'usuari està autentificat i té assignat el Rol necessari per accedir a cada URL que sol·liciti.

El problema que s'ha detectat és provocat perquè Acegi, al comparar la URL introduïda per l'usuari amb la llista d'URLs protegides, utilitza la URL complerta, inclosos els paràmetres i els seus valors.

Aprofitant aquesta característica, és possible afegir un paràmetre amb un valor que faci que l'algorisme de comparació d'URLs no vegi la URL introduïda com una de les protegides i, per tant, en permeti l'accés sense autentificació.

Estan afectades totes les aplicacions que utilitzin una llibreria d'Acegi (acegi-security-x.y.z.jar) amb versió anterior a la 1.0.2 i tinguin, en la definició de URLs protegides, determinats tipus de patró. Com que aquestes condicions són les utilitzades per defecte en les aplicacions desenvolupades tant amb openFrame 1.x com amb Canigó 2.x, cal considerar totes les aplicacions desenvolupades amb aquests entorns com a potencialment afectades.

Solució proposada

La solució proposada consisteix en fer que la validació d'URLs no tingui en compte els paràmetres i els seus valors, descartant per tant tot el que pugui haver-hi després del primer "?".

Aquesta solució ja ha estat implementada i provada en les darreres versions d'Acegi (a partir de la 1.0.2) i Spring Security (a partir de la 2.0.4) i el que s'ha fet per part de l'Oficina és portar-la a les versions anteriors utilitzades en Canigó i openFrame.

Correcció del problema en aplicacions en producció

Per tant, la correcció consisteix en substituir, en cada aplicació, la llibreria d'Acegi

- Canigó 1.x i Canigo 2.x amb versió inferior a 2.2:
    - substituir `acegi-security-0.8.3.jar` per `acegi-security-0.8.3.canigo.patch.jar`
- Canigó 2.x amb versió superior igual o superior a 2.2:
    - substituir `acegi-security-0.9.0.jar` per `acegi-security-0.9.0.canigo.patch.jar`

Aquestes es poden descarregar de la corresponent adreça del repositori maven2 de Canigó:

http://canigo.ctti.gencat.net/repository/maven2/acegisecurity/acegi-security/0.8.3.canigo.patch/

http://canigo.ctti.gencat.net/repository/maven2/acegisecurity/acegi-security/0.9.0.canigo.patch/

Perquè la substitució sigui efectiva, caldrà reiniciar l'aplicació o el servidor d'aplicacions, verificant que la llibreria antiga no estigui ni en l'aplicació ni en els caches del servidor d'aplicacions.

Amb aquesta solució, **no cal fer cap modificació en el codi o configuració** de les aplicacions desplegades en els entorns de Producció, Preproducció o Integració. La utilització dels patrons de URL afectats pel problema continua sent vàlida i ja no comporta el risc que s'ha descrit.

En l'entorn de desenvolupament corresponent caldrà aplicar el procediment descrit en l'apartat "Correcció del problema en aplicacions en desenvolupament" aquest mateix document.

Problema amb l'autentificació d'usuaris en Aplicacions Desenvolupades amb Canigó

Possibles problemes

Si en una aplicació s'han definit patrons de URL en els que intervenen els noms o valors de paràmetres, deixaran de funcionar amb aquesta correcció perque aquestes dades ja no es tenen en compte al ver la validació.

Aquest tipus de configuració és poc probable i s'ha de considerar una mala pràctica. Si es dona el cas, es recomana replantejar la configuració del servei de seguretat per que no depengui dels paràmetres i aplicar la correcció descrita.

Per diagnosticar si en una aplicació es pot donar aquest problema, car revisar l'arxiu `canigo-services-security.xml / openframe-services-security.xml.` Concretament en la definició de la propietat secureUrls dins el bean authorizationConfiguration no hi ha d'haver cap URL que contingui el caràcter "?" o el nom o valor d'un paràmetre.

Correcció del problema en aplicacions en desenvolupament

La correcció en les aplicacions en desenvolupament passa igualment per substituir la llibreria afectada (Acegi) per la llibreria que conté el fix desenvolupat per la Oficina Tècnica de Canigó.

Projectes ja iniciats construïts amb maven

En el repositori de Canigó s'ha publicat el paquet afectat:

- **Canigó 1.x o Canigó 2.x amb versió inferior a 2.2:**
  - groupId: acegisecurity
  - artifactId: acegi-security
  - versió: 0.8.3.canigo.patch
- **Canigó 2.x amb versió igual o superior a 2.2:**
  - groupId: acegisecurity
  - artifactId: acegi-security
  - versió: 0.9.0.canigo.patch

Procés d'aplicació per maven 2 (Canigo 2.x i Canigo 1.4-Snapshot):

La estructura natural d'un projecte Canigó conté en el pom.xml un referència al projecte canigo-root com a parent:

```
<parent>
      <artifactId>canigo-root</artifactId>
      <groupId>canigo</groupId>
      <version>2.3.3</version>
</parent>
```

Si es disposa d'aquesta entrada, només caldrà assegurar que estem treballant de forma on-line. Si es així el projecte canigo-root de totes les versions ha estat modificat per tal que contingui la corresponent referència a la versió corregida d'Acegi.

Si no es disposa d'aquesta entrada, s'ha fet una modificació a la estructura recomanada del projecte. En aquest cas i amb la supervisió de l'arquitecte de l'aplicació s'ha d'afegir la dependència a primer nivell de la versió corregida d'acegi (0.8.3.canigo.patch o 0.9.0.canigo.patch) segons toqui:

```
<dependency>
      <groupId>acegisecurity</groupId>
      <artifactId>acegi-security</artifactId>
      <version>0.9.0.canigo.patch</version>
</dependency>
```

Procés d'aplicació per maven 1 (Canigo 1.x menys Canigo.1.4-Snapshot):

Versions inferiors a 1.4-Snapshot no són recomanades per desenvolupament.

En cas de estar fer servir aquesta versió s'ha de modificar el fitxer *project.properties* substituint:

version.acegi=0.8.3

per

version.acegi=0.8.3.canigo.patch

També s'ha de verificar que en el fitxer *project.xml* la versió d'Acegi està correctament associada al fitxer de propietats:

```
<dependency>
      <groupId>acegisecurity</groupId>
      <artifactId>acegi-security</artifactId>
      <version>${version.acegi}</version>
      <type>jar</type>
      <properties>
            <war.bundle>true</war.bundle>
      </properties>
</dependency>
```

Projectes ja iniciats construïts sense maven

En els projectes en que no es faci servir maven per la construcció i que per tant tinguin una llista estàtica de llibreries associades al projecte només caldrà substituir el .jar original d'acegi pel nou .jar:

- Canigó 1.x i Canigo 2.x amb versió inferior a 2.2:
    - substituir `acegi-security-0.8.3.jar` per `acegi-security-0.8.3.canigo.patch.jar`
- Canigó 2.x amb versió superior igual o superior a 2.2:
    - substituir `acegi-security-0.9.0.jar` per `acegi-security-0.9.0.canigo.patch.jar`

Aquestes es poden descarregar de la corresponent adreça del repositori maven2 de Canigó:

http://canigo.ctti.gencat.net/repository/maven2/acegisecurity/acegi-security/0.8.3.canigo.patch/

http://canigo.ctti.gencat.net/repository/maven2/acegisecurity/acegi-security/0.9.0.canigo.patch/

Projectes nous

En aquest apart es considera com a projecte nou, aquell que s'inicia a partir de la plantilla de Canigó publicada i no d'un projecte ja existent.

En aquest projecte la versió d'Acegi a fer servir ve determinada per la referència al projecte parent:

```
<parent>
      <artifactId>canigo-root</artifactId>
      <groupId>canigo</groupId>
      <version>2.3.3</version>

</parent>
```

I per tant no cal fer cap pas addicional.

Verificació de la solució

Poden activar-se les traces a la classe on hi ha el problema original i sobre la que s'ha implementat la correcció afegint

```
<category name="net.sf.acegisecurity.intercept.web.PathBasedFilterInvocationDefinitionMap">
    <level value="debug"/>
</category>
```

a la configuració de log4j.

No és convenient deixar activada aquesta configuració de forma permanent en un entorn de producció perquè pot generar un volum relativament elevat de traces i afegir en els arxius de traces informació que hauria d'estar protegida.

Amb aquestes traces activades, es pot verificar que s'ha instal·lat correctament la llibreria amb la correcció perquè, a l'introduir una URL amb paràmetres, es traça la operació que els elimina i en les següents operacions de comparació s'utilitza la URL "neta" sense paràmetres.

Per exemple:

```
- Strip query string, from: '/AppJava/categories.do?reqCode=search&nouParametre=unValor'; to:
'/AppJava/categories.do'
- Converted URL to lowercase, from: '/appjava/categories.do'; to: '/appjava/categories.do'
- Candidate is: '/appjava/categories.do'; pattern is /**; matched=true
- Strip query string, from: '/AppJava/categories.do?reqCode=search&nouParametre=/unValor'; to:
'/AppJava/categories.do'
- Candidate is: '/AppJava/categories.do'; pattern is /AppJava/pagelogin.do* ; matched=false
- Candidate is: '/AppJava/categories.do'; pattern is /**/files.do ; matched=false
- Candidate is: '/AppJava/categories.do'; pattern is /**/categories* ; matched=true
```

En una aplicació afectada pel problema es pot verificar que un cop aplicada la solució, l'accés no autoritzat ja no ha de ser possible i l'intent de fer-ho ha de portar cap a la pantalla que demana el codi d'usuari i la clau d'accés.

Referències

Bugs reportats en el sistema de gestió d'incidències d'Acegi i Spring

- SEC-161: http://jira.springframework.org/browse/SEC-161
- SEC-321: http://jira.springframework.org/browse/SEC-321
- SEC-953: http://jira.springframework.org/browse/SEC-953