**Description**

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

**Solution**

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

## Passaggio 1: Scaricare e Installare la Versione Aggiornata di Tomcat

1. **Scarica la versione aggiornata di Tomcat** dal sito ufficiale di Apache Tomcat:
   - Apache Tomcat 7.0.100
   - Apache Tomcat 8.5.51
   - Apache Tomcat 9.0.31
2. **Esegui il backup della tua configurazione corrente** e delle applicazioni Web per sicurezza.
3. **Estrarre l'archivio Tomcat** nella directory desiderata. Ad esempio:

tar -xvzf apache-tomcat-9.0.31.tar.gz -C /opt/

4.**Aggiorna i collegamenti simbolici (se necessario) per puntare alla nuova versione di Tomcat:**

sudo ln -sfn /opt/apache-tomcat-9.0.31 /opt/tomcat

**5.Aggiorna i permessi della directory di Tomcat se necessario:**

sudo chown -R tomcat:tomcat /opt/apache-tomcat-9.0.31

## Passaggio 2: Configurare il Connettore AJP

Per migliorare la sicurezza del connettore AJP, aggiorna il file `server.xml` di Tomcat. Aggiungi l'attributo `secretRequired` e configura un segreto.

1. **Apri il file `server.xml`** nella directory di configurazione di Tomcat (di solito in `/opt/tomcat/conf/server.xml`):

sudo nano /opt/tomcat/conf/server.xml

2. **Trova il connettore AJP** (solitamente qualcosa di simile a `<Connector port="8009" protocol="AJP/1.3" />`) e aggiornalo per includere l'attributo `secretRequired="true"` e `secret="yourSecret"`. Ad esempio:

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"

secretRequired="true" secret="mySecretPassword" />

**3.Riavvia Tomcat** per applicare le modifiche:

```
sudo systemctl restart tomcat
```

## Passaggio 3: Aggiornare il Connettore Web Server (ad esempio, Apache HTTPD) per Utilizzare il Segreto AJP

Se stai utilizzando un web server come Apache HTTPD con `mod_proxy_ajp`, devi aggiornare la configurazione per includere il segreto.

1. **Apri il file di configurazione di Apache** (di solito in `/etc/httpd/conf/httpd.conf` o `/etc/apache2/sites-available/000-default.conf`):

```
sudo nano /etc/httpd/conf/httpd.conf
```

**2.Aggiorna il proxy AJP** per includere il segreto. Ad esempio:

```
<Proxy "ajp://localhost:8009">
    Require all granted
    ProxyPass "ajp://localhost:8009" secret="mySecretPassword"
</Proxy>
```

<Proxy "ajp://localhost:8009">

Require all granted

ProxyPass "ajp://localhost:8009" secret="mySecretPassword"

</Proxy>

**3.Riavvia Apache** per applicare le modifiche:

sudo systemctl restart httpd

## Passaggio 4: Verifica

1. **Verifica che Tomcat stia funzionando correttamente** e che il connettore AJP richieda il segreto configurato.
2. **Testa la connessione AJP** tramite il web server per assicurarti che la configurazione del segreto funzioni come previsto.

## Riepilogo

Seguendo questi passaggi, avrai aggiornato il server Tomcat alla versione più recente e configurato il connettore AJP per richiedere l'autorizzazione con un segreto. Questo migliorerà la sicurezza della tua configurazione Tomcat e ridurrà la possibilità di accessi non autorizzati tramite il connettore AJP.