Wie werden Apache-, Tomcat- und andere Drittanbieter-Anwendungsversionen auf Cisco Security Manager überprüft?

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Version der verschiedenen Cisco Security Manager (CSM)-Komponenten überprüft wird.

Hintergrundinformationen

Cisco Security Manager (CSM) erfordert nur wenige serverseitige Komponenten, nämlich Apache Web Server, Tomcat Servlet Engine usw.

Diese serverseitigen Komponenten verfügen über eigene Anwendungsversionen. Bei jeder neuen Version von CSM kann sich die Anwendungsversion ändern. Daher muss manchmal gekreuzt werden, ob sich eine drohende Sicherheitslücke oder CVE auf die Komponentenversion ODER im Wesentlichen auf die Version von Cisco Security Manager auswirkt.

Überprüfen der Anwendungsversion von Apache, Tomcat und anderen Drittanbietern in Cisco Security Manager

Dies kann über die Eingabeaufforderung cmd oder Power Shell unter Windows Server überprüft werden.

Tomate

```
java -cp C:\Progra~2\CSCOpx\MDC\tomcat\lib\catalina.jar org.apache.catalina.util.ServerInfo

C:\Users\Administrator>java -cp C:\Progra~2\CSCOpx\MDC\tomcat\lib\catalina.jar
org.apache.catalina.util.ServerInfo
Server version: Apache Tomcat/6.0.44
Server built: Aug 10 2015 04:28:32 UTC
Server number: 6.0.44.0
OS Name: Windows NT (unknown)
OS Version: 10.0
Architecture: x86
JVM Version: 1.7.0_121-b31
JVM Vendor: Oracle Corporation
```

Apache

```
C:\>Apache.exe -version
Server version: Apache/2.4.23 (Win32) Server built: Oct 1 2016 11:19:05
```

JAVA

```
C:\>java.exe -version
java version "1.7.0_121"
Java(TM) SE Runtime Environment (build 1.7.0_121-b31)
Java HotSpot(TM) Client VM (build 24.121-b31, mixed mode)
```

OpenSSL

```
C:\>openssl
WARNING: can't open config file: c:\ciscossl/ssl/openssl.cnf
OpenSSL> version
CiscoSSL 1.0.2j.6.1.140-fips
```

Hinweis: Die oben genannten Ausgaben stammen von der Version Cisco Security Manager 4.13.