Apache Cassandra JMX/RMI Remote Code Execution

17/04/2015

Software:	Cassandra
Affected Versions:	Cassandra 1.2.0 - 1.2.19 Cassandra 2.0.0 - 2.0.13 Cassandra 2.1.0 - 2.1.3
CVE Reference:	CVE-2015-0225
Author:	Georgi Geshev - MWR Labs (https://labs.mwrinfosecurity.com/)
Severity:	High
Vendor:	Apache Software Foundation
Vendor Response:	Fix Released

Description

Apache Cassandra is an open source distributed database management system. Cassandra is designed to handle large amounts of data across many commodity servers with no single point of failure.

Apache Cassandra was found to bind an unauthenticated JMX/RMI service on all network interfaces. An adversary with network access may abuse this service and achieve arbitrary remote code execution as the running user.

Impact

An attacker may achieve arbitrary code execution with the privileges of the user running Cassandra on the remote system.

Cause

The default installation of Apache Cassandra binds an unauthenticated JMX/RMI service on all available network interfaces.

Interim Workaround

This vulnerability can be mitigated by enabling authentication for the JMX/RMI endpoint, reconfiguring the service to bind on localhost or completely disabling the service.

The following lines will enable JMX authentication when added to Cassandra's startup shell script.

```
JVM_OPTS="$JVM_OPTS -Dcom.sun.management.jmxremote.authenticate=true"

JVM_OPTS="$JVM_OPTS -Dcom.sun.management.jmxremote.password.file=/etc/cassandra/jmxremote.password"
```

Solution

Users of Apache Cassandra 2.0.X should upgrade to version 2.0.14, whilst users of 2.1.X need to upgrade to version 2.1.4.

Technical details

Java Management Extensions (JMX) technology provides a simple and standard way of managing and monitoring resources related to an instance of a Java Virtual Machine (JVM). This is achieved by instrumenting resources with Java objects known as Managed Beans (MBeans) that are registered with an MBean server.

Apache Cassandra was found to bind a JMX/RMI service by default. This service was exposed without authentication and available on all network interfaces.

```
# ps faxuwww | grep cass | grep -v grep
115      10076 18.9 80.7 492736 415604 ?       SLl  12:44   1:16 java […]
-Dcom.sun.management.jmxremote.port=7199 -Dcom.sun.management.jmxremote.rmi.port=7199
-Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false […]
org.apache.cassandra.service.CassandraDaemon
# netstat -anvlp 2>/dev/null | grep 10076
tcp        0      0 127.0.0.1:9160          0.0.0.0:*               LISTEN      10076/java
tcp        0      0 127.0.0.1:9042          0.0.0.0:*               LISTEN      10076/java
tcp        0      0 127.0.0.1:7000          0.0.0.0:*               LISTEN      10076/java
tcp        0      0 0.0.0.0:39224           0.0.0.0:*               LISTEN      10076/java
tcp        0      0 0.0.0.0:7199            0.0.0.0:*               LISTEN      10076/java
unix  2      [ ]         STREAM     CONNECTED     38891    10076/java
unix  2      [ ]         STREAM     CONNECTED     38760    10076/java
#
```

A remote adversary could craft and deploy a malicious MBean that would subsequently be served from a Management Applet (MLet) that is hosted on an attacker controlled HTTP server. The JMX agent will load the MLet, fetch the MBean and execute the attacker's code.

Detailed Timeline

Date:	Summary:
21/01/2015	Vulnerability is reported to Apache
27/01/2015	Apache confirms reception
26/03/2015	Apache suggests fix
01/04/2015	Public fix released
15/04/2015	Advisory published