Cisco Cloud Web Security Connector JMX/RMI Remote Code Execution

17/04/2015

Software:	Cloud Web Security Connector
Affected Versions:	Cloud Web Security Connector 3.0.1.2
CVE Reference:	CVE-2015-0689 (this CVE was registered by Cisco and confirmed by them to be associated with this vulnerability)
Author:	Apostolis Mastoris - MWR Labs (http://labs.mwrinfosecurity.com/)
Severity:	High
Vendor:	Cisco
Vendor Response:	Fix Released

Description

Cisco Cloud Web Security (CWS) is a Software-as-a-Service solution which offers scanning and filtering capabilities on user requested Internet traffic. CWS filters out content that is inappropriate or does not conform to a defined policy. Cisco CWS Connector acts as a proxy to redirect the web traffic to CWS service.

Cisco CWS Connector running on Microsoft Windows systems ships with its own Java Runtime Environment (JRE) and exposes a Java Management Extensions (JMX) interface that does not require authentication. A vulnerability exists in CWS Connector which allows unauthenticated users to gain unauthorised access with administrative privileges on the target host.

Impact

An unauthenticated attacker who is able to access the port on which the JMX interface is exposed can use this flaw to achieve Remote Code Execution (RCE). The service runs with “SYSTEM” privileges on a Microsoft Windows operating system and thus an adversary may gain complete control of the host.

Cause

The default installation of CWS Connector version 3.0.1.2 on Microsoft Windows includes and uses its own JRE 1.6 which has a JMX endpoint enabled by default that does not require authentication.

Interim Workaround

Enable the on host firewall to prevent access to the JMX interface on TCP port 1099.

Solution

Upgrade to Cisco CWS Connector 3.0.1.7 or later versions.

Technical details

On Microsoft Windows operating systems, CWS Connector 3.0.1.2 ships with JRE v1.6. The default deployment of CWS Connector on Windows exposes a JMX endpoint on TCP port 1099. In addition, the JMX interface is not configured to require authentication.

A JMX agent provides the capability to remotely manage and monitor Java applications running on the Java Virtual Machine (JVM). Due to the lack of authentication, a user could craft their own Managed Beans (MBeans) and execute arbitrary code through the Java application served on the JVM.

The CWS Connector application is executed as a Windows service in the context of the “NT AUTHORITY\SYSTEM” user. An attacker capable of executing code through the exposed JMX endpoint could gain administrative access, fully compromising the confidentiality, integrity, and availability of the host.

Detailed Timeline

Cisco acknowledged the issue and a CVE ID was assigned (CVE-2015-0689).

Date:	Summary:
17/11/2014	Reported to Cisco.
17/11/2014	Cisco confirmed reception.
12/12/2014	MWR InfoSecurity requested current status.
12/12/2014	Cisco confirmed that a PSIRT case id has been assigned and awaited action from an incident manager.
06/01/2015	Cisco requested further information on the issue.
20/01/2015	MWR InfoSecurity provided additional information, however no response was received.

10/02/2015	MWR InfoSecurity confirmed that the issue has been fixed on latest version (3.0.1.9). CWS Connector release notes mention that JMX has been disabled since 3.0.1.7, however no notification from Cisco was provided.
24/02/2015	MWR InfoSecurity contacted Cisco again, however no response was received.
30/03/2015	MWR InfoSecurity contacted Cisco again. Cisco informed MWR InfoSecurity that the issue will be investigated.
06/04/2015	Cisco verified the issue, assigned a CVE and released an advisory on their portal.
10/04/2015	Cisco requested a co-ordinated public release and MWR received confirmation from Cisco that the CVE was associated with the issue reported.
17/04/2015	Advisory published.