MWR LABS

Security Advisory

Arcserve Unified Data Protection JMX/RMI Remote Code Execution

17/03/2017

Software	Unified Data Protection (UDP)
Affected Versions	UDP versions 5 and 6
CVE Reference	CVE-2016-9927
Author	Apostolis Mastoris – MWR Labs (https://labs.mwrinfosecurity.com)
Severity	High
Vendor	Arcserve
Vendor Response	Fix Released

Description

Arcserve Unified Data Protection (UDP) suite provides functionality for data protection for critical data and applications. The suite protects data stored in cloud, virtual and physical infrastructure and supports configuration and management of all aspects of data protection through a single user console.

Arcserve UDP installation on Microsoft Windows was found to expose an unauthenticated JMX/RMI service on the underlying system's network interface. An adversary with network access may abuse this service and achieve arbitrary remote code execution with administrative privileges on the target host.

Impact

An attacker may achieve arbitrary code execution with the privileges of the user running UDP on the remote system. By default 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 the UDP console version 5 and 6 on Microsoft Windows exposes a JMX endpoint enabled by default that does not require authentication.

Interim Workaround

Users of Arcserve UDP versions 5 and 6 can apply the following configuration to remediate the issue:

1. Access the following registry key:

```
HEKY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\
CAARCAppSvc\Parameters\Java
```

2. Right click on the registry key at the right-hand panel, select “Modify...” and the “Edit Multistring” window will appear.
3. Remove the following parameters:

```
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8086
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmx.authenticate=false
```

4. Restart Arcserve UDP Management Service.

Further information is provided at the following URL:

- https://arcserve.zendesk.com/hc/en-us/articles/217506966

Solution

Users of Arcserve UDP 5 and 6 should upgrade to version 6.5.

Technical details

The default deployment of UDP on Microsoft Windows exposes a JMX endpoint on TCP port 8086. 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.

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
2016-11-25	Issue reported to vendor.
2016-11-30	Vendor acknowledged the issue.
2016-12-14	Vendor published interim workaround for the issue.
2017-01-31	Updated version including the patch was released.
2017-03-17	Advisory published.