Aleph JBoss Vulnerability

- **Article Type:** General
- **Product:** Aleph
- **Product Version:** 20

Description:
This KB is only relevant for customers on Aleph SP 20.2.5 and lower. It is not relevant for customers using Aleph SP 20.2.6 and higher.

After finding evidence of port scanning from Ex Libris services, we identified the cause was a worm (a form of malware) that uses a JBoss vulnerability to scan ports and create processes on the server, which may create a system load and is of course a security hazard. The vulnerability only exists for customers using port 80 or 8080, but a future generation of such a worm may infect those using other ports as well.

JBOSS is normally only used by Aleph with the Restful APIs, Aleph Web Services, and to support OPAC via Primo. We have not found any Aleph customers infected by this worm to date, but we are making this announcement as a precaution to explain how to protect Aleph. If you are not running JBOSS then your risk is reduced, but we still strongly recommend that you apply the fix.

Attack Details & Fix Instructions

A worm is exploiting a security exposure in the JBoss jmx-console installed on the Aleph application. Using an HTTP HEAD request the worm bypasses the existing exposure mitigation and installs the web application zecmd (or iesvc). This application allows for the execution of arbitrary commands as the Aleph user. Using zecmd or iesvc, the worm downloads and extracts a package and starts a copy of the worm.

The worm is a Perl script that masks itself as another process. It first starts another Perl script, an IRC server, that also masks itself as another process. The worm then compiles a port scanner and begins scanning a random Class B subnet of IP addresses looking for JBoss servers on some set of ports. For every JBoss server found it attempts to propagate itself as described above.

To prevent infection, the jmx-console web application must be un-deployed. This is accomplished by moving jmx-console.war out of the Aleph JBoss deployment directory (/exlibris/aleph/a??_?/ng/aleph/home/system/thirdparty/openserver/server/default/deploy). The zecmd (or iesvc) web application, if installed, can be found in the management sub-directory (/exlibris/aleph/a??_?/ng/aleph/home/system/thirdparty/openserver/server/default/deploy/management) and should be deleted. If infected, the processes mentioned above (the worm, the IRC server, and the port scanner) should be killed. Finally the JBoss bin directory (/exlibris/aleph/ a??_?/ng/aleph/home/system/thirdparty/openserver/bin), needs to be cleaned up. All worm packages should be removed, as well as any file they extracted.

Customers may use these to prevent and/or remove an infection. We have also created a script to address this issue by making the changes outlined above. The script is attached to this KB Item as jmx297360.zip. Download this zip file to your Aleph application server, unzip, and execute the file inside with the command, "ksh jmx297360.ksh", as the root user. It will log its activity to the screen and under the Aleph root directory, to the file /exlibris/aleph/a??_?/ng/aleph/home/system/thirdparty/openserver/server/default/log/jmx297360.log You may contact Support if you need any assistance.

We have seen the following variations of this worm:
kisses.tar.gz (v1)
Scans port 80
Masks itself as
/usr/local/jboss/bin/tomcat
/usr/local/apache/bin/httpd –DSSL
Port Scanner: pnscan
kisses.tar.gz (v2)
Scans ports 80 & 8080
Masks itself as
/usr/local/jboss/bin/tomcat
/usr/local/apache/bin/httpd –DSSL
Port Scanner: pnscan

Resolution:

- **Article last edited:** 10/8/2013