Addressing CVE-2020-1938 Tomcat vulnerability for Voyager Environments

- **Product:** Voyager
- **Product Version:** All
- **Relevant for Installation Type:** Multi-Tenant Direct, Dedicated-Direct, Local, TotalCare

---

CVE-2020-1938 vulnerability was reported when using Apache JServ Protocol (AJP)

This Impacts Apache Tomcat 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 , Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses.

This issue can be addressed in Voyager by downloading and running the patch kit on the voyager server.

This procedure requires:

- Access to the exlibirs FTP server at downloads.exlibrisgroup.com
- Access to the root user on your system.
- Basic understanding of the linux command line.

If uncomfortable with or unable to run the following commands please open a case to Voyager support:

Installing Patch for CVE-2020-1938 in Voyager Environments

1. Log on to the server as root.
2. Run the following commands:

```
mkdir -p /m1/incoming/patch

cd /m1/incoming/patch

ftp downloads.exlibrisgroup.com

voyager / LVf_,7lF

cd patch

mget *

exit

bzip2 -dc vik4.patch.tar.bz2 | tar -xvf -
```

3. Launch the Voyager patch kit with these commands:

```
cd vik4
./ikit_menu
```

4. Run menu 1 steps 1 through 5, 7, 8 and 10 to download the latest 3rd party packages for Voyager, including the new

Tomcat

5. Run menu 2 steps 1 through 5 and 16 and 17. These will stop Apache and Voyager, install the latest versions of your 3rd party packages and then re-start Apache and Voyager.

- **Article last edited:** 3/16/2020