ImageMagick Security Issue CVE-2016–3714 "ImageTragick"

ImageMagick is a third party application used by Rosetta to manipulate image files. Here we explain how to mitigate ImageMagick Security Issue CVE-2016–3714 "ImageTragick"

Explanation of the threat

This vulnerability can lead to remote code execution if specially constructed image files are submitted.

See: https://imagetragick.com/

In most cases Rosetta will mitigate the threat as the presence of the appropriate "Magic Byte" sequence in image files will be ensured by the validation stack, however to completely mitigate the threat it is necessary to disable the vulnerable coders in the ImageMagick configuration.

How to disable the vulnerable coders

The following lines should be added to this configuration file:

```
/exlibris/product/ImageMagick-6.6.1-10/lib/ImageMagick-6.6.1/config/policy.xml
```

```
<policymap>
  <policy domain="coder" rights="none" pattern="EPHEMERAL" />
  <policy domain="coder" rights="none" pattern="URL" />
  <policy domain="coder" rights="none" pattern="HTTPS" />
  <policy domain="coder" rights="none" pattern="MVG" />
  <policy domain="coder" rights="none" pattern="MSL" />
  <policy domain="coder" rights="none" pattern="TEXT" />
  <policy domain="coder" rights="none" pattern="SHOW" />
  <policy domain="coder" rights="none" pattern="WIN" />
  <policy domain="coder" rights="none" pattern="PLT" />
</policymap>
```