

# Imagemagick

Security hole recently detected and published in imagemagick.

More info:

<http://www.theregister.co.uk/2016/05/03/imagemagick/><sup>[1]</sup>

<https://imageragick.com/><sup>[2]</sup>

And updated files in ubuntu 14.04.x or centos 7.x. based OS's.

How to patch affected systems:



```
sudo nano /etc/ImageMagick/policy.xml
```

and add the policies within the appropriate section <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="HTTP" />
  <policy domain="coder" rights="none" pattern="FTP" />
  <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" />
  <policy domain="coder" rights="none" pattern="LABEL" />
  <policy domain="path" rights="none" pattern="@*" />
```

## BBB

<https://groups.google.com/forum/#!topic/bigbluebutton-setup/s5zeNpg5M8I><sup>[3]</sup>



Hi all,

We use ImageMagick as a dependency in the BigBlueButton. We expect that Canonical will be updating the ImageMagick package very soon, but in the mean time your BigBlueButton servers have a vulnerable version of the package installed.

The vulnerability can be exploited by uploading a crafted "png" or "jpg" file that actually contains an SVG or MSL file with exploit code as a presentation.

We *strongly recommend* everyone update the policy.xml file as described

<https://imageragick.com/#info>

Specifically, add the following:

```
<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" />
```

to

```
/etc/ImageMagick/policy.xml
```

For example

```
<policymap>
  <!-- <policy domain="system" name="precision" value="6"/> -->
  <!-- <policy domain="resource" name="temporary-path" value="/tmp"/>
-->
  <!-- <policy domain="resource" name="memory" value="2GiB"/> -->
  <!-- <policy domain="resource" name="map" value="4GiB"/> -->
  <!-- <policy domain="resource" name="area" value="1GB"/> -->
  <!-- <policy domain="resource" name="disk" value="16EB"/> -->
  <!-- <policy domain="resource" name="file" value="768"/> -->
  <!-- <policy domain="resource" name="thread" value="4"/> -->
  <!-- <policy domain="resource" name="throttle" value="0"/> -->
  <!-- <policy domain="resource" name="time" value="3600"/> -->
  <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" />
</policymap>
```

There is no need to restart your BigBlueButton server. Once you edit the policy.xml your version of ImageMagick is no longer vulnerable.

*\*We recommend that anyone running BigBlueButton (or any other server that uses imagemagic) do this now. \**

Regards, ... Fred & Calvin

---

<sup>[1]</sup> <http://www.theregister.co.uk/2016/05/03/imagemagick/>

<sup>[2]</sup> <https://imageragick.com/>

<sup>[3]</sup> <https://groups.google.com/forum/#!topic/bigbluebutton-setup/s5zeNpg5M8I>