Invenio-files-rest XSS security fix

Invenio Developer Forum 22. May 2017

Nicolas Harraudeau

INVENIO

The vulnerability

Invenio

http://invenio.com/api/files/<BUCKET_ID>/myfile.html

Malicious code executed under the Invenio instance domain.

How?

- Invenio Files REST was serving files which could have MIME types like ‘text/html’ or ‘application/javascript’.

- The browser was then rendering those files.

- The files’ URLs contain the Invenio instance’s domain, thus they can perform any action using the user’s session.

The current FIX

A **new option** was added to **by default serve any file as untrusted** which will prevent the browser from rendering files (e.g. HTML). The principle is that images and audio will be served with correct type; **text files, whether it's plain text, html, css, javascript or JSON will be served as text/plain**; **everything else will be served as application/octet-stream**. Further **HTTP headers** will be sent to prevent content type sniffing from browsers.

Which versions are fixed

- https://github.com/inveniosoftware/invenio-files-rest/pull/151/commits/2114fff879cebf39198f2cacb01f2999933e5ff6
- Merged in invenio-files-rest 1.0.0a16 and 1.0.0a14-post1

Possible long term FIX

The best solution is to **serve user uploaded files from a another domain** (not a subdomain) so that malicious files can only target other user uploaded files, not the whole API.

Your TODO

- If you have allowed user uploaded files, you should **check all files to see if anybody exploited this XSS vulnerability**.
- **Update your version of invenio-files-rest**.

Thanks for the FIX

The issue was found by the Zenodo team and fixed by Lars Holm Nielsen.

Appendix:
Which Headers are used

See https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers

```
# Prevent loading resources like JavaScript from any source
headers['Content-Security-Policy'] = "default-src 'none';"

# Prevent MIME type sniffing for browser.
headers['X-Content-Type-Options'] = 'nosniff'

# Prevent opening of downloaded file by IE
headers['X-Download-Options'] = 'noopen'

# Prevent cross domain requests from Flash/Acrobat.
headers['X-Permitted-Cross-Domain-Policies'] = 'none'

# Prevent files from being embedded in frame, iframe and object tags.
headers['X-Frame-Options'] = 'deny'

# Enable XSS protection (IE, Chrome, Safari)
headers['X-XSS-Protection'] = '1; mode=block'
```