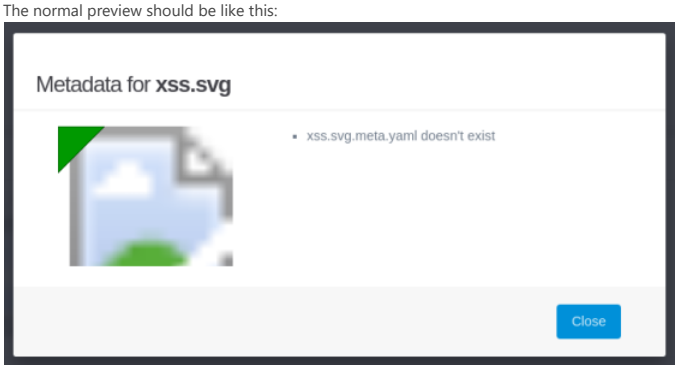
Cross-site Scripting (XSS) - Stored in getgrav/grav-plugin-admin

0

Valid Reported on Oct 27th 2021

Description

In Grav, you can preview the file you uploaded by hovering your mouse to the file and clicking the info icon.
The normal preview should be like this:



However, I noticed that it is possible to perform XSS on the filename due to the following HTML Code:

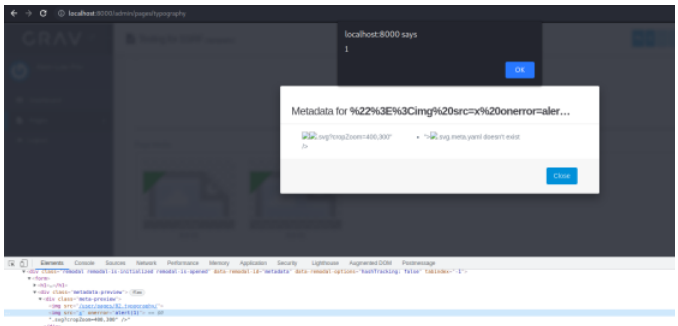
```
<div class="meta-preview">
    <img src="/user/pages/02.typography/xss.svg?cropZoom=400,300">
</div>
```

We can upload a file with a filename of `"><img src=x onerror=alert(1)>` and it will escape the quote for the `src` parameter and execute our XSS payload.
Rendered HTML Code:

```
<div class="meta-preview">
    <img src="/user/pages/02.typography/">
    <img src="x" onerror="alert(1)">
    .svg?cropZoom=400,300" />;
</div>
```

Aside from that, I also found that the meta-content is also vulnerable when returning the error message.

```
<div class="meta-content">
    <ul>
        <li>
            <strong></strong>
            " ">"
            <img src="x" onerror="alert(1)">
            .svg.meta.yaml doesn't exist
        </li>
    </ul>
</div>
```



Proof of Concept

Upload a file with `"><img src=x onerror=alert(1)>` as filename
Click the Metadata or info icon of the uploaded file

Impact

A malicious user could execute JS code and target other users of the website by retrieving their details such as Admin-Nonce, IP address, User Agent, Current Page Content, etc.

CVE
CVE-2021-3920
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (4.6)

Visibility
Public

Status
Fixed

Found by

Aj Dumanhug
@ajdumanhug
unranked

Fixed by

Matias Griese
@mahagr
maintainer

This report was seen 428 times.

We have contacted a member of the **getgrav/grav-plugin-admin** team and are waiting to hear back a year ago

Aj Dumanhug a year ago Researcher

I also noticed that when I deleted the file. The notification alert will also execute JS Code.

Aj Dumanhug modified the report a year ago

Aj Dumanhug modified the report a year ago

Aj Dumanhug modified the report a year ago

Aj Dumanhug modified the report a year ago

Aj Dumanhug a year ago Researcher

Updates:

Added data that can be retrieved by attacker

Added a screenshot showing the data being retrieved when the victim opened the metadata of the file

Fix CVSS

We have sent a follow up to the **getgrav/grav-plugin-admin** team. We will try again in 7 days. a year ago

A **getgrav/grav-plugin-admin** maintainer a year ago — Maintainer

Can you please update repository to point to https://github.com/getgrav/grav-plugin-admin ?

Aj Dumanhug a year ago — Researcher

Hi! I'm sorry I don't have a privilege to edit the target repository. Maybe the @admin can.

Djamil Legato a year ago — Maintainer

As this is not a Grav issue but an Admin issue, we find ourselves unable to mark this as valid even though it technically is and already working on a fix.

If someone can point it to https://github.com/getgrav/grav-plugin-admin that would be appreciated

Matias Griese validated this vulnerability a year ago

Aj Dumanhug has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

Jamie Slome a year ago — Admin

Sorted! 🎉

Matias Griese marked this as fixed with commit **646313** a year ago

Matias Griese has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

Jamie Slome a year ago — Admin

CVE published! 🎊

Matias Griese a year ago — Maintainer

Thank you!