XSS In MoinMoin When Uploading A SVG File With Malicious Javascript Code In Its Content

PYTHON MOIN XSS


Catarina Leite Nov 8, 2020

Details Overview

Summary

MoinMoin before version 1.9.11 is vulnerable to a Cross Site Scripting attack. An attacker with write permissions can upload a `SVG` file that contains `malicious javascript`. This malicious code will be executed in the victim's browser when the victim is viewing that SVG file on the wiki.

Product

MoinMoin before 1.9.11

Impact

Malicious javascript code will be executed in the victim's browser.

Steps To Reproduce

```
1. With MoinMoin running, go to the home page and create a new page.
2. Save the changes on this new page and go to the attachments section.
3. Upload a SVG file that contains the following malicious code in its content:
    >>> <script type="text/javascript">
    >>> alert('XSS by Checkmarx');
    >>> </script>
4. Click on the view option.
```

Expected Result:

An alert box will be displayed with the text "XSS by Checkmarx"

Remediation

Update MoinMoin to 1.9.11 and above

Credit

This issue was discovered and reported by Catarina Leite from the CxSCA AppSec team at Checkmarx.

Resources

1. Advisory
2. Commit 64e1603