New issue

Jump to bottom

Cross-site Scripting (XSS) and HTML Injection on ClearCanvas ImageServer 3.0 Alpha #227

Open **JoshuaProvoste** opened this issue on Jul 24, 2019 · 3 comments

JoshuaProvoste commented on Jul 24, 2019

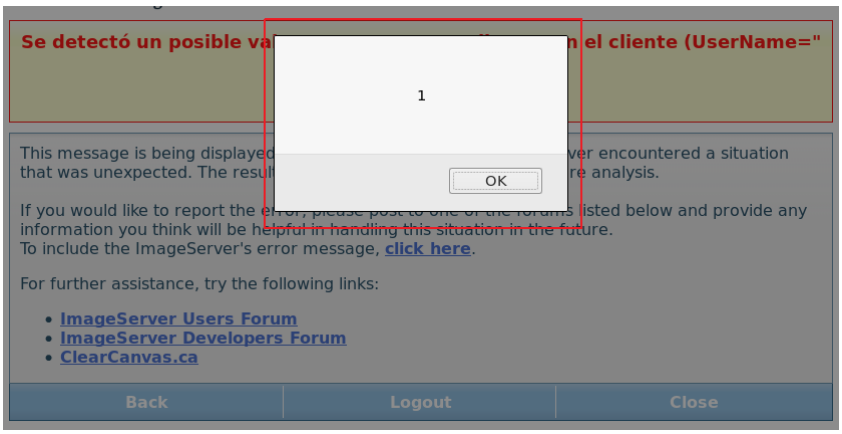
Hello,

I found two vulnerabilities that affect to ClearCanvas ImageServer 3.0 Alpha:

- Cross-site Scripting (XSS) reflected
- HTML Injection

You can reproduce both with the following details,

1. Payload: <p/onclick=alert(1)>xss
2. Vulnerable POST data: &UserName=<p/onclick=alert(1)>xss
3. Output: A potentially dangerous Request.Form value was detected from the client (UserName="<p/onclick=alert(1)>...").
4. Step 1: Open /ImageServer/Pages/Login/Default.aspx or /Pages/Login/Default.aspx URL login page according your config deployments
5. Step 2: Fill the username and password inputs with XSS/HTML payload and submit the login form.
6. Step 3: Then, you will have a XSS/HTML injections clicking on payload.



If you need reproduce, fix the issue, or more details about that, please, feel free to ping me.

steveTree commented on Jul 25, 2019

can you confirm the version
am assuming you are talking about v13.2? have you tested it on the original version ?

JoshuaProvoste commented on Jul 25, 2019 Author

I talk about this ClearCanvas version:

IDELGADO9 commented on Feb 11, 2020

i need clear canvas imageserver 3.0 alpha, please share it with me.... thanks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants