


Genesys PureConnect - Interaction Web Tools XSS

2022.09.15

 **Jake Murphy - Echelon Risk + Cyber**
(<https://cxsecurity.com/author/Jake+Murphy+-+Echelon+Risk+%2B+Cyber/1/>). (US) 

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **CVE-2022-37775**
(<https://cxsecurity.com/cveshow/CVE-2022-37775/>)

CWE: **N/A**

Dork: (See Dorks List) inurl:"/l3Root/chatOrCallback.html"
(<https://cxsecurity.com/dorks/>)

Product: Genesys PureConnect - Interaction Web Tools Chat Service

Description: Interaction Web Tools Chat Service allows XSS within the Printable Chat History via the participant -> name JSON POST parameter.

Vulnerability Type: XSS

Vendor of Product: Genesys PureConnect

Affected Product Code Base: Interaction Web Tools - Chat Service -
Appears to be all versions up to current release (26-September-2019)

Affected Component: "Print" feature of the Interaction Web Tools Chat
at: https://help.genesys.com/pureconnect/mergedprojects/wh_tr/desktop/pdfs/web_tools_dg.pdf

Attack Vectors:

- To exploit the Cross-Site Scripting vulnerability, visit <https://<vulnerable-domain>/I3Root/chatOrCallback.html>
- Then select the 'I don't have an account' option, and enter the name "><script>alert(1)</script>"
- Then press 'Start Chat'
- Then enter anything in the chat box like 'asdfg' and press send
- Now select the 'Printable Chat History' in the top right corner
- XSS will trigger. You can google dork for vulnerable versions with `inurl:"/I3Root/chatOrCallback.html"`

I'm assuming if an admin tries to print the chat conversation, it will trigger for them as well. Unable to confirm though.

References:

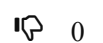
<http://genesys.com>
<http://interaction.com>

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2022090038>).

Tweet

Lubię to!

Vote for this issue:



50%

50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)