


Reflected Cross Site Scripting on Import People

By: Rivera Rivera

user

13 Feb 2020 at 2:53 a.m. CST

8 Responses



I have identified that it is possible to execute JavaScript code on Import People functionality.

STEPS TO REPRODUCE: You have to create a file with the following filename: ">.xlsx

When you try to upload this file, the alert will be executed.

HOW TO FIX: Apply output encoding to filename parameter.

REFERENCES: https://owasp.org/www-project-cheat-sheets/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet (https://owasp.org/www-project-cheat-sheets/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet)

Gluu 4.0

Ubuntu 18.04

closed

Answers

By Rivera Rivera

user

19 Feb 2020 at 4:03 a.m. CST

Copy




This vulnerability is also exploitable on Import/Export Attributes functionality using a file with the following filename: ">.ldif

By Aliaksandr Samuseu

staff

19 Feb 2020 at 8:16 a.m. CST

Copy



Hi, Rivera.

Do you mean these features can be used without getting authenticated first at web UI? Otherwise it's not clear how this can be utilized by somebody except the servcies's administrators.

That said, it still doesn't feel right that text in a file's name can be treated as line of code (still seems as a minor web UI bug to me, not a security threat).


@Thomas Gasmr.Mougang could you fix it?

By Rivera Rivera

user

19 Feb 2020 at 10:12 a.m. CST

Copy



Hi Aliaksandr,

It could be only exploitable once you are authenticated, so as you said, only service's administrator could exploit the vulnerability.


Best regards.

By Thomas Gasmr Mougang

staff

19 Feb 2020 at 4:31 p.m. CST

Copy



@Aliaksandr.Samuseu I'm closing this ticket.

By Rivera Rivera

user

20 Feb 2020 at 2 a.m. CST

Copy




Hi @Thomas Gasmr.Mougang In which Gluu version do you plan to fix this issue?

By Thomas Gasmr Mougang

staff

20 Feb 2020 at 3:05 a.m. CST

Copy




This is not a security issue. Also that component will be replace in 4.2.

By Rivera Rivera

user

20 Feb 2020 at 3:28 a.m. CST

Copy



This is a self-xss vulnerability, you can review the following reference to understand the risks associated to this vulnerability: <https://silentbreaksecurity.com/weaponizing-self-xss/> (<https://silentbreaksecurity.com/weaponizing-self-xss/>)

Anyway, are you planning to replace both components? (Import People and Import/Export Attributes)



Rivera,
This is open source project, you can contribute directly and we will check the merge request.

Post an answer

You need to [Login \(/authorize/?next=tickets_url/other/7992/reflected-cross-site-scripting-on-import-people/\)](/authorize/?next=tickets_url/other/7992/reflected-cross-site-scripting-on-import-people/) in order to post an answer

[Company \(http://www.gluu.org/company/our-story/\)](http://www.gluu.org/company/our-story/)

[Partners \(http://www.gluu.org/partners/overview/\)](http://www.gluu.org/partners/overview/)

[News \(http://news.gluu.org\)](http://news.gluu.org)

[Blog \(http://www.gluu.org/blog/\)](http://www.gluu.org/blog/)

[Support \(https://support.gluu.org/\)](https://support.gluu.org/)

[Documentation \(http://gluu.org/docs\)](http://gluu.org/docs)

Press Releases

[View All \(http://www.gluu.org/resources/press-releases/\)](http://www.gluu.org/resources/press-releases/)

Last Tweets

[Follow Us \(https://twitter.com/GluuFederation\)](https://twitter.com/GluuFederation)

The Gluu Daily is out! <https://t.co/SRcmjgRELk> Stories via @opensourceway @mariadb @realpython

The Gluu Daily is out! <https://t.co/FHHI14sbEF> Stories via @CenDemTech @fabiomoioli @pewresearch

Questions?

SCHEDULE A DEMO
([HTTP://GLUU.YOUCANBOOK.ME](http://gluu.youcanbook.me))

