paatui / README.md

CVE-2020-18327

README.md

Alfresco Community Edition v5.2.0 – Reflected XSS vulnerability in Administration Console

Description

Alfresco is a collection of information management software products for Microsoft Windows and Unix-like operating systems developed by Alfresco Software Inc. using Java technology.

Reflected Cross Site Scripting (XSS) vulnerability exists in Alfresco Community Edition v5.2.0 via the action parameter in the alfresco/s/admin/admin-nodebrowser API, which allows a remote attacker to inject arbitrary JavaScript.

Date: 03 March 2022
Software Link: https://www.alfresco.com
Exploit Author: Chakrit Sangsakul, Pongpol Phaiaroonrut, Thanavit Chongsutakawewong
CVE: CVE-2020-18327
Category: Web Application

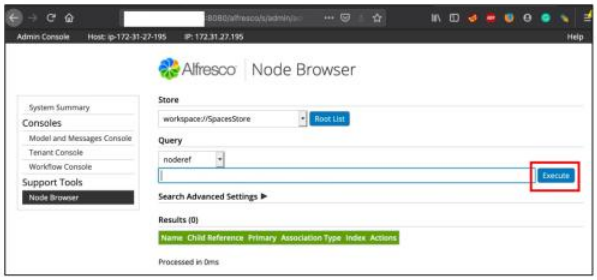
Proof of Concept

1. Access to Alfresco Administration Console.
2. Navigate to “Node Browser” function in “Support Tools” and querying the Node browser by pressing the “Execute“ button.
3. Inject JavaScript into “action” parameter.

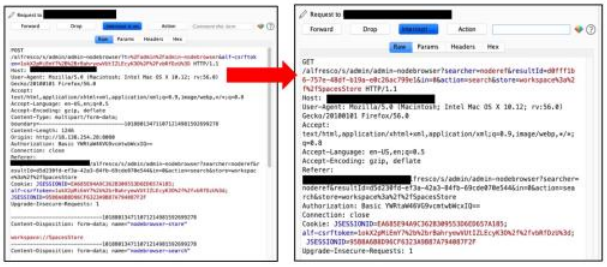
Alfresco Authenticated Reflected Cross-Site Script (XSS) PoC

1. Access and login as "admin" user in the "Alfresco Administration Console (admin only)" menu.

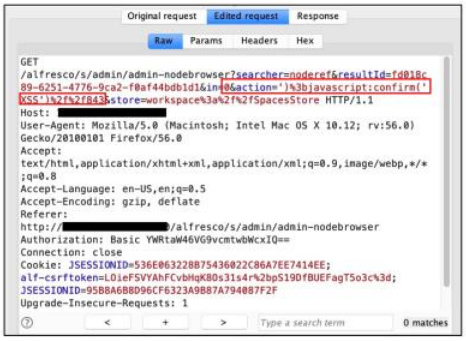
2. Navigate to "Node Browser" function in "Support Tools" and querying the Node browser by pressing the "Execute" button.



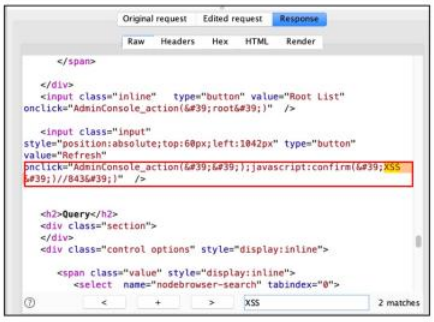
3. When "execute" button was accessed, tester used the HTTP proxy to intercept the HTTP request.



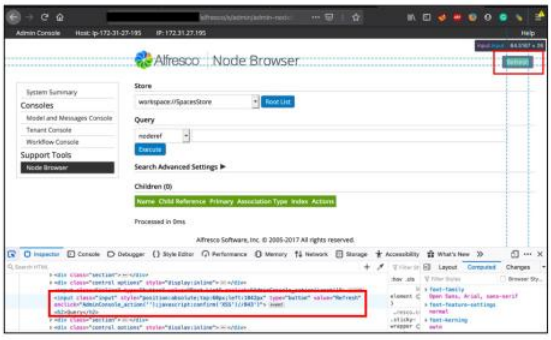
4. Tester manipulated the "action" parameter and change the value to JavaScript payload. For example, the confirm() method was used to identify the XSS vulnerability.

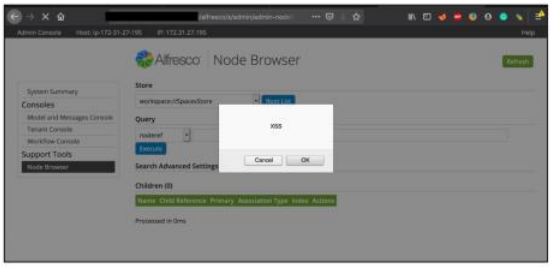


5. After HTTP request was sent, I have inspected the XSS payload was sent successfully.



6. To prove the Reflected XSS vulnerability, "Refresh" button must be clicked to trigger the onclick() method. Finally, the XSS confirmation pop-up was shown.





Timeline

Discovery and report : 24 June 2019
CVE ID was assigned : 11 Aug 2021
Public : 3 March 2022

Solution

- Update Alfresco Community Edition to version v6.2 or later
- Consider complying to the OWASP's XSS prevention guidelines. (https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)