

Developers Blog

This is a personal blog for two users, here we share all the problems which we face in our daily life during penetration testing activities or during other software development activities. Further you can ask us any question regarding our posts in comments.

Joplin App Desktop Version Vulnerable to XSS



By [Aamir Rehman](#) - May 11, 2021

Dear Reader Jubair Rehman Yousafzai Here:

Update Sept 2022: CVE assigned CVE-2021-33295

<https://www.cvedetails.com/cve/CVE-2021-33295/>

During the testing of Joplin App Desktop Version before 1.8.5 I was able to execute the malicious XSS when entered in Main body of Joplin App Desktop,

Once I click on Toggle button twice, the payload was executed successfully.

The payload which I have used for this testing is as below

```
<noscript><p title="</noscript><img src=x onerror=alert('testing')">
```

Below is the POC for this exploit

After reporting to the Joplin team they fixed the issue directly and released the fixed in 1.8.5 version.

Below are their release notes and details:

<https://github.com/laurent22/joplin/releases/tag/v1.8.5>

Thanks

Jubair Rehman: <https://twitter.com/jubairfolder>



To leave a comment, click the button below to sign in with Google.



Popular posts from this blog

Ericsson BSCS iX R18 Billing & Rating (ADMX, MX) - Stored XSS

By [Aamir Rehman](#) - January 30, 2020



Dear Reader, I was able to identify stored XSS in multiple web base modules of Ericsson BSCS iX R18 Billing & Rating platform Below are its details: # Software description: Ericsson Billing is a convergent billing solution for telecoms that combines an unrivaled combination of out-of-the box features and high

[READ MORE](#)

Autoconfiguration ipv4 address 196.254.x.x IP Problem

By [Aamir Rehman](#) - April 12, 2013



Today when i connect my laptop to Lan it wasn't getting the ip from my DHCP server. Instead it gives me some weird IP like 196.254.x.x . while my Wifi was working fine, I searched Alot to get to know until i found a great piece of code on a blog. so going to share with you guys. Problem with my lq ...

[READ MORE](#)

ZKT Eco ADMS - Stored XSS

By [Aamir Rehman](#) - September 27, 2022



Hi All, I was able to identify stored XSS in one online attendance system i.e. ZKT Eco ADMS (v 3.1-164) (Automatic Data Master Server) is a powerful web-based time and attendance management software. which is used to configure the attendance devices and manage its users. Cve ID assigned ...

[READ MORE](#)

 Powered by Blogger

Theme images by [Michael Elkan](#)



Contributors



AAMIR REHMAN



ASAD ULLAH

Subscribe Us via email

Enter your email address:
















[Subscribe](#)

Archive

GHDB For any Website

example.com

Type in your domain & Click
Below Links

-  [APIs Leak via Postman](#)
-  [Publicly exposed documents](#)
-  [Directory listing vulnerabilities](#)
-  [Configuration files exposed](#)
-  [Database files exposed](#)
-  [Log files exposed](#)
-  [Backup and old files](#)
-  [Login pages](#)
-  [SQL errors](#)
-  [PHP errors/warnings](#)
-  [phpinfo\(\)](#)
-  [Search Pastebin.com](#)
-  [Search Github/Gitlab](#)
-  [Search Stackoverflow](#)
-  [Signup pages](#)