Easily Exploitable Critical Vulnerability in ProfilePress Plugin of WordPress CVE-2021-34621

Published by Numan Rajkotiya at September 8, 2021

SecureLayer7
Time and Again, Securing You
Easily Exploitable Critical Vulnerability in ProfilePress Plugin

Understanding the Vulnerability

ProfilePress, formerly WP User Avatar, a WordPress plugin installed on over 400,000 sites made it possible for an attacker to upload arbitrary files to a vulnerable site and register as an administrator on sites even if user registration was disabled, all without requiring any prior authentication which could lead to site takeover.

During the user registration process, users could supply arbitrary user metadata that would get updated during the registration process. This included the **wp_capabilities** user meta that controls a user's capabilities and role.

What is wp_capabilities?

The official WordPress documentation describes the capability as the permission to perform one or more types of tasks. The key "wp_capabilities" is present in the database table **wp_usermeta** which identifies the serialized representation of an array that identifies a user's roles and any capabilities that have been added to that user with $user->add_cap('my_capability');

This made it possible for a user to supply wp_capabilties as an array parameter while registering, which would grant them the supplied capabilities, allowing them to set their role to any role they wanted, including administrator.

ddition, there was no check to validate that user registration was enabled on the site, making it possible for users to register as an administrator e ites where user registration was disabled. This meant that attackers could completely take over a vulnerable WordPress site without much effort erable version of this plugin is in use. or

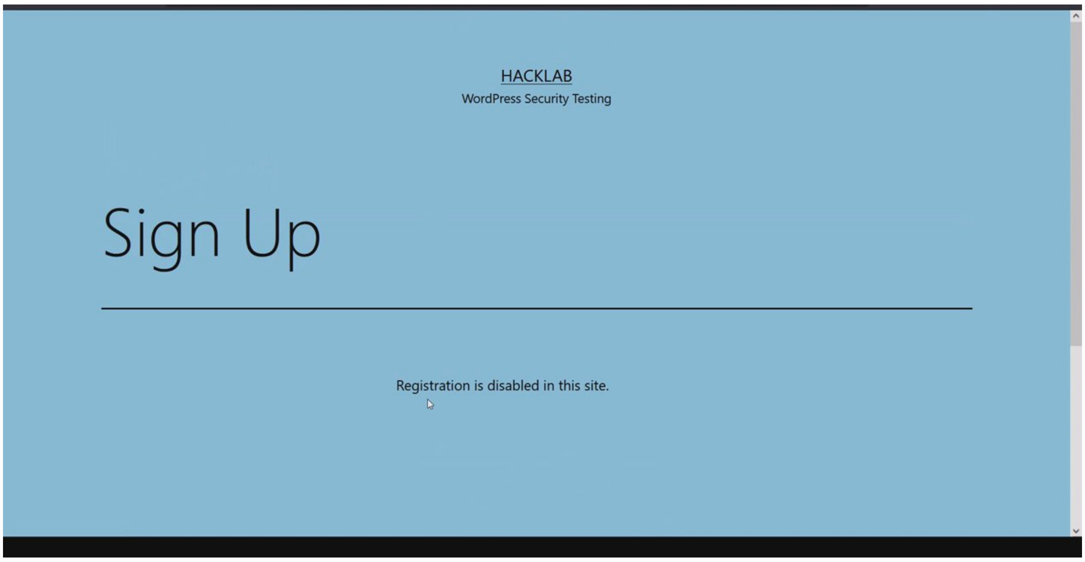
This function takes the user input data in the form of an array i.e name=**"wp_capabilities[administrator]"**, the whole array is stored in the $user_data variable.

These critical and easily exploitable security issues have been patched, therefore, we highly recommend updating to the latest patched version available, 3.1.16, immediately if you are running a vulnerable version of this plugin (3.0 – 3.1.3)

In order to exploit the vulnerability, the registration function should be called with the wp_capabilities array with administrator value.

Proof of Concept

The request to endpoint "/wp-admin/admin-ajax.php" can be exploited even if registration is disabled on a vulnerable site by adding an extra parameter **"wp_capabilities[administrator]=1"** as payload to the request which escalates the user's privilege to the administrator.



HACKLAB

WordPress Security Testing

Sign Up

Registration is disabled in this site.

The following exploit can be downloaded from here.

Upon successful exploitation, a new account is created with administrative privilege:

Conclusion

To keep your WordPress website secure, you will have to update the ProfilePress Plugin version to the latest one. You can download the latest version from here. If you're seeking help to patch this vulnerability, you can always contact at info@securelayer7.net

Reference:

www.wordfence.com/blog/2021/06/easily-exploitable-critical-vulnerabilities-patched-in-profilepress-plugin/

Share

Numan Rajkotiya

Numan Rajkotiya is an Intern security consultant at SecureLayer7 with some intense liking towards the technical field. Along with an ambitious development at hand, he is currently expanding his expertise with committed work proficiency.

Related posts

August 29, 2021

Cybersecurity webinar On-Demand Penetration Testing with BugDazz

Read more

July 8, 2021

Importance of Cryptography Encryption in Apps & Latest Encryption Algorithm

Read more

April 21, 2021

Latest cybersecurity trends in 2021 amid Covid-19 Pandemic

Read more

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Quick Links

- Home
- About
- Blog
- News
- Contact Us

Services

- Application Security
- Network Security
- Mobile Application Security
- Thick Client Security
- VoIP Penetration Testing

Security Expertise

- IoT Device Security
- ICO Security
- Web Malware Removal
- Red Teaming Assessment

Network Security

- Telecom Security Assessment
- Server Hardening
- Wireless Security Assessment
- Firewall Configuration Review

General

- Privacy Policy
- Disclaimer Agreement
- Terms of Use
- Usage Agreement