Back to all articles
UPDATED: 11.10.2021

Critical Security Vulnerability Fixed In WP Reset PRO

Dave
from **patchstack**

Table of Contents

There was a critical security vulnerability in the WP Reset PRO plugin which allowed any authenticated user to wipe the database.

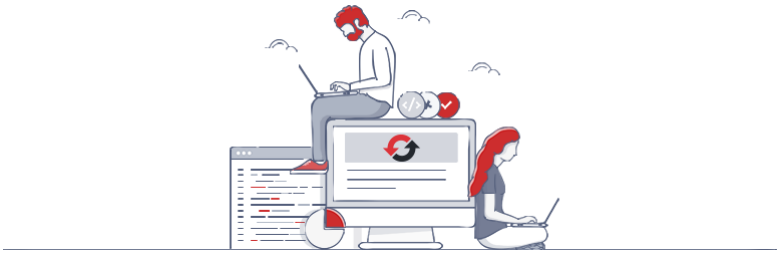
Do you want to be the first to be alerted about such vulnerabilities? Sign up for Patchstack Community (Free) plan and monitor up to 99 websites for free.

For plugin developers, we have security audit services and Threat Intelligence Feed API for hosting companies.

The PRO version of the WP Reset plugin (versions 5.98 and below) suffers from a vulnerability that allows any authenticated user, regardless of their authorization, to wipe the entire database.

Because it wipes all tables in the database, it will restart the WordPress installation process which could allow an attacker to launch this installation process and then create an administrator account at the end of this process as by default an administrator account has to be created once the WordPress site has been installed.

After this, they could further exploit the site by uploading a malicious plugin or uploading a backdoor.



The plugin is described as a plugin that helps you to quickly reset the site's database to the default installation values without modifying any files. It deletes all customizations and content or just chosen parts like theme settings.

The described issue was fixed in version 5.99 after a rapid response (within 24 hours!) by the developer team of the plugin in question.

The security vulnerability in WP Reset PRO plugin

The issue in this plugin is caused due to a lack of authorization and nonce token check. The plugin registers a few actions in the *admin_action_** scope. In the case of this vulnerability, it's *admin_action_wpr_delete_snapshot_tables*.

Unfortunately, the *admin_action_** scope does not perform a check to determine if the user is authorized to perform said action, nor does it validate or check a nonce token to prevent CSRF attacks.

This action is registered as follows:

The function delete_snapshot_tables looks like the following:

```
function delete_snapshot_tables($uid = '')
{
    global $wpdb;

    if (empty($uid)) {
        $uid = $_GET['uid'];
    }

    if (strlen($uid) != 4 && strlen($uid) != 6) {
        return new WP_Error(1, 'Invalid UID format.');
    }

    $tables = $wpdb->get_col($y = $wpdb->prepare('SHOW TABLES LIKE %s', array($uid . '
    foreach ($tables as $table) {
        $wpdb->query('DROP TABLE IF EXISTS `' . $table . '`');
        if ($wpdb->last_error !== '') {
            $this->log('error', 'Failed to delete table ' . $table . ': ' . $wpdb->las
        } else {
            $this->log('info', 'Deleted table ' . $table);
        }
    }

    if (!empty($_GET['redirect'])) {
        wp_safe_redirect($_GET['redirect']);
    }

    return true;
}
```

It can be seen that the *uid* query parameter is grabbed from the URL, which is directly used as a prefix of the tables that should be deleted. Since the LIKE operator is used, we can pass a query parameter such as *%%wp* to delete all tables with the prefix wp.

Once this is done, someone could simply visit the homepage of the site to start the WordPress installation process.

The patch in WP Reset PRO

Since this is a premium plugin, the patch cannot be seen at the WordPress.org SVN repository.

Based on our own research and communication with the development team of the WP Reset PRO plugin, we can confirm that an authentication and authorization check has been added using the current_user_can function, along with a check to determine if a valid nonce token is present in the request using the check_admin_referer function.

In addition to this, the *uid* query parameter is also checked and made sure that it's a string only containing letters using the ctype_alpha function.

Timeline

27-09-2021 - We discovered the vulnerability in WP Reset PRO and released a virtual patch to all Patchstack paid version customers.
27-09-2021 - We reached out to the developer of the plugin.
28-09-2021 - The developer replied and we provided the vulnerability information.
28-09-2021 - The developer released a new plugin version, 5.99, which fixes this issue.
10-11-2021 - Published the article.
10-11-2021 - Added the vulnerability to the Patchstack vulnerability database.

Websites with Patchstack paid version are protected from the issue and have received a virtual patch.

Get latest WordPress security insight from our **Patchstack Weekly** series

Start listening

Related Articles

View All >

WORDPRESS SECURITY VULNERABILITIES

Most Common WordPress Plugin Vulnerabilities & How to Fix Them

LAST PATCH, WORDPRESS PLUGIN SECURITY

Patching an Arbitrary User Creation Security Bug in "thecartpress" Plugin

PATCHSTACK WEEKLY

Patchstack Weekly #51: How One Vulnerability Affects Many

Documentation

Patchstack

About us

Careers

Media kit

Articles & insight

Whitepaper 2021

Social

LinkedIn

Facebook

Twitter

hackuu

Join Discord