Chloe Chamberland

January 16, 2020

Easily Exploitable Vulnerabilities Patched in WP Database Reset Plugin

On January 7th, our Threat Intelligence team discovered vulnerabilities in WP Database Reset, a WordPress plugin installed on over 80,000 websites. One of these flaws allowed any unauthenticated user to reset any table from the database to the initial WordPress set-up state, while the other flaw allowed any authenticated user, even those with minimal permissions, the ability to grant their account administrative privileges while dropping all other users from the table with a simple request.

These are considered critical security issues that can cause complete site reset and/or takeover. **We highly recommend updating to the latest version (3.15) immediately.** Wordfence Premium users have been protected from these vulnerabilities since January 8th with a custom firewall rule. Wordfence free users will receive the same protection on February 7th.

Description: Unauthenticated Database Reset
Affected Plugin: WP Database Reset
Affected Versions: <= 3.1
CVE ID: CVE-2020-7048
CVSS Score: 9.1 (Critical)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
Patched Version: 3.15

WP Database Reset is an easy to use database reset plugin that provides users with the ability to reset any database tables on their site to the same state as a fresh WordPress install. This is handy for administrators doing testing on their website and for administrators who want to start over without requiring a complete WordPress re-installation. This plugin provides a powerful feature that, if left unprotected, could wreak havoc for site owners. Unfortunately, that was exactly what we found in this plugin.

None of the database reset functions in the plugin were securely protected with capability checks or security nonces. Without proper security controls in place, the WP Database Reset plugin contained a serious flaw that allowed any unauthenticated user the ability to reset any table in the database. This reset would result in a complete loss of data availability. An attacker could send a simple request and a site would be completely reset to the WordPress standard defaults.

Vulnerable version of the plugin code:

```
public function reset( array $tables ) {
         if ( in_array('users', $tables ) ) {
           $this->reset_users = true;
         }

         $this->validate_selected( $tables );
         $this->set_backup();
         $this->reinstall();
         $this->restore_backup();
       }

       private function validate_selected( array $tables ) {
         if ( ! empty( $tables ) && is_array( $tables ) ) {
           $this->selected = array_flip( $tables );
```

Revised version of the plugin code with security nonce check and capability check in place:

```
public function reset(array $tables)
{
  if (wp_verify_nonce(@$_REQUEST['submit_reset_form'], 'reset_nounce') && current_user_can('administrator')) {
     // Check if current user is Admin and check the nonce

    if (in_array('users', $tables)) {
      $this->reset_users = true;
    }

    $this->validate_selected($tables);
    $this->set_backup();
    $this->reinstall();
    $this->restore_backup();
  } else {
    throw new Exception(__('Please reload the page and try again. Double check your security code.', 'wordpress-databa
  }
}
```

A WordPress database stores all data that makes up the site including posts, pages, users, site options, comments, and more. With a few simple clicks and a couple of seconds, an unauthenticated user could wipe an entire WordPress installation clean if that installation was using a vulnerable version of this plugin.

Description: Privilege Escalation
Affected Plugin: WP Database Reset
Affected Versions: <= 3.1
CVE ID: CVE-2020-7047
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Patched Version: 3.15

To further escalate the previous vulnerability, any user authenticated as a subscriber and above had the ability to reset the `wp_users` table. Initially, this doesn't seem too severe. Dropping all users during a database reset may be problematic, but we can always recreate users, right? Unfortunately, this was more complex. Whenever the `wp_users` table was reset, it dropped all users from the user table, including any administrators, except for the currently logged-in user. The user sending the request would automatically be escalated to administrator, even if they were only a subscriber. That user would also become the only administrator, thus allowing an attacker to fully take over the WordPress site.

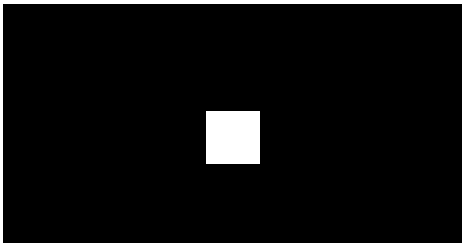
```
private function update_user_settings() {
 global $wpdb;



   $wpdb->prepare(
    "UPDATE $wpdb->users
     SET user_pass = '%s', user_activation_key = ''
     WHERE ID = '%d'",
     $this->user->user_pass, $user_id
   )
 );

 if ( $this->reset_users ) {
   wp_clear_auth_cookie();
   wp_set_auth_cookie( true );
 }
}
```

A site owner allowing open registration on a site with a vulnerable version of the WP Database Reset plugin could lose control of their site. Here's a demonstration of how this exploit would work.



Reminder: Backup Your WordPress Site

This vulnerability serves as an important reminder that [maintaining site backups] is an incredibly important component to maintaining the security and availability of your site. Some compromises require [professional clean up] or incident response and forensic investigation. Without backups, even professional remediation wouldn't be helpful after a compromise like this. Backups can also improve recovery time in the event of a compromise. We recommend that site owners:

- Backup regularly in intervals. Once a week would be a good place to start.
- Backup every time a major change is made on the site.
- Store backups on a server or device separate from WordPress installations. That way the integrity of your backup can be trusted in the event that the site or its server becomes compromised.

Disclosure Timeline

January 7th, 2020 – Vulnerability initially discovered and analyzed.
January 8th, 2020 – Full details disclosed to plugin developer and custom firewall rule released to Wordfence premium users.
January 13th, 2020 – Developer responds and notifies us that a patch will be released the next day.
January 14th, 2020 – Patch released.
January 16th, 2020 – Public disclosure.

Conclusion

In today's post, we detailed two severe vulnerabilities discovered in the WP Database Reset plugin. These flaws are patched in version 3.15. **If you have this plugin installed on your site, we urge you to update immediately.**

Sites running [Wordfence Premium] have been protected from any attacks against these vulnerabilities since January 8th. Free users will receive the same protection on February 7th.

Did you enjoy this post? Share it!

Comments

1 Comment

Internet Marine *
January 16, 2020
1:23 pm

Many thanks for all you people do.

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service   Privacy Policy

CCPA Privacy Notice

Products
- Wordfence Free
- Wordfence Premium
- Wordfence Care
- Wordfence Response
- Wordfence Central

Support
- Documentation
- Learning Center
- Free Support
- Premium Support

News
- Blog
- In The News
- Vulnerability Advisories

About
- About Wordfence
- Careers
- Contact
- Security
- CVE Request Form

Stay Updated

you@example.com

□ By checking this box I agree to the terms of service and privacy policy *

SIGN UP