Security Advisory 2020-009

Critical Vulnerability in ThemeGrill Demo Importer Wordpress Plugin

February 19, 2020 — v1.0

TLP:WHITE

History:

- *19/02/2020 — v1.0 – Initial publication*

Summary

A critical vulnerability affecting the ThemeGrill Demo Importer plugin has been identified [1, 2]. Theme Grill Demo Importer is a plugin that can be used to import ThemeGrill official themes demo content, widgets and theme settings [2]. The plugin is affected by a vulnerability that allows any unauthenticated user to *wipe the entire database* to its default state after which they are automatically logged in as an *administrator*. According to [2], there are more than 100K active installations of the plugin.

Technical Details

Prerequisites:

In order for the vulnerability to be exploitable, there must be a theme installed and activated by ThemeGrill. In order to be automatically logged in as an *administrator*, there must be a user called `admin` in the database. If the `admin` user does not exist in the database, then the users table will remain empty and there will be no automatic login.

Details:

Once the plugin detects that a ThemeGrill theme is installed and activated, it loads the file `/includes/class-demo-importer.php` which hooks `reset_wizard_actions` into `admin_init`. The `admin_init` hook runs not only in the admin environment, but also on calls to `/wp-admin/admin-ajax.php` which does not require a user to be authenticated [1].

The bug is present in the `reset_wizard_actions` function where there is no authentication check [1]. If the user is not logged in, the `admin` user object will be retrieved from WordPress and then all WordPress tables that start with the defined WordPress database prefix will be dropped.

Once all tables have been dropped, it will populate the database with the default settings and data after which it will set the password of the `admin` user to its previously known password.

Products Affected

List of affected products:

WordPress ThemeGrill Importer plugin versions between (and including) 1.3.4 and 1.6.1

Recommendations

It is highly recommended to update the plugin to the latest version as soon as possible. This vulnerability has been fixed in versions 1.6.2 and above.

References

[1] https://www.webarxsecurity.com/critical-issue-in-themegrill-demo-importer/

[2] https://wordpress.org/plugins/themegrill-demo-importer/