Ram Gall

October 26, 2021

Site Deletion Vulnerability in Hashthemes Plugin

Update: a previous version of this article incorrectly indicated that this vulnerability could be used for site takeover, we have updated this for accuracy, as the impact is instead complete loss of site content.

Note: To receive disclosures like this in your inbox the moment they're published, you can subscribe to our WordPress Security Mailing List.

On August 25, 2021, the Wordfence Threat Intelligence team initiated the disclosure process for a vulnerability in Hashthemes Demo Importer, a WordPress plugin with over 7,000 installations.

This vulnerability allowed any authenticated user to completely reset a site, permanently deleting nearly all database content as well as all uploaded media.

As we did not receive a response from the developer for nearly a month, we contacted the WordPress plugins team with our disclosure on September 20, 2021. The plugin was temporarily removed from the repository the same day, and a patched version, 1.1.2, was made available on September 24, 2021, though it was not mentioned in the developer changelog.

Wordfence Premium customers received a firewall rule protecting against this vulnerability on August 25, 2021. Sites running the free version of Wordfence received the same rule 30 days later, on September 24, 2021.

Description: Improper Access Control allowing content deletion
Affected Plugin: Hashthemes Demo Importer
Plugin Slug: hashthemes-demo-importer
Plugin Vendor: Hashthemes
Affected Versions: <= 1.1.1
CVE ID: CVE-2021-39333
CVSS Score: 8.1(High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
Researcher/s: Ramuel Gall

The Hashthemes demo importer plugin failed to perform capability checks for many of its AJAX actions. While it did perform a nonce check, the AJAX nonce was visible in the admin dashboard for all users, including low-privileged users such as subscribers. The most severe consequence of this was that a subscriber-level user could reset all of the content on a given site.

Any logged-in user could trigger the `hdi_install_demo` AJAX function and provide a `reset` parameter set to `true`, resulting in the plugin running it's `database_reset` function. This function wiped the database by truncating every database table on the site except for `wp_options`, `wp_users`, and `wp_usermeta`. Once the database was wiped, the plugin would then run its clear_uploads function, which deleted every file and folder in `wp-content/uploads`.

Timeline

August 25, 2021 – Wordfence Threat Intelligence finishes our investigation and attempts to initiate disclosure for a vulnerability in HashThemes Demo Importer. We release a firewall rule to Wordfence Premium customers.
September 20, 2021 – We contact the WordPress plugins team as we have not received a response from the plugin developer. The plugin is temporarily removed from the WordPress.org repository.
September 24, 2021 – A patched version of the plugin, 1.1.2, becomes available. The firewall rule becomes available to free Wordfence users.

Conclusion

In today's post, we discussed a vulnerability in HashThemes Demo Importer that allowed any logged-in user to completely and permanently destroy all of the content on a website.

We've discussed the importance of backups in the past, and this vulnerability serves as an important reminder of how critical backups are to your site's security. While most vulnerabilities can have destructive effects, it would be impossible to recover a site where this vulnerability was exploited unless it had been backed up.

Wordfence Premium users have been protected against this vulnerability since August 25, 2021, while those still running the free version of Wordfence have been protected since September 24, 2021. If you are running a vulnerable version of this plugin, we urge you to update to the latest version available, 1.1.4, as soon as possible.

If you know a friend or colleague who is using this plugin on their site, please forward this advisory to them to help keep their sites protected as this vulnerability can lead to complete loss of site content.

Did you enjoy this post? Share it!

Comments

6 Comments

Marek *
October 26, 2021
7:45 am

This is only to say how grateful I feel for you for making the net safer. Many thanks

Jhorman Duban Rodriguez Pulgarin *

October 26, 2021
8:08 am

media." and then in the conclusion, it reads: "In today's post, we discussed a vulnerability in HashThemes Demo Importer that allowed any logged-in user to completely and permanently destroy all of the content on a website.

*

Ram Gall *
October 26, 2021
8:47 am

Hi,
Authenticated users are logged-in users. This does not allow un-authenticated users to delete site contents.
Thanks

Sachin Palewar *
October 26, 2021
11:22 pm

Hi @Jhorman, Just to go into more details. It means any user so for example on a simple Wordpress sites, you have have users with just subscriber access. Those are just your readers of blogs, even they will be able to do it so basically it doesn't mean authenticated users limit anyone. As most websites have certain roles which are really available to anyone who signs-up. With Woocommerce websites, it can be even serious as all the buyers, when they sign-up, get the customer role assigned to them. You can even register as a customer without even buying anything. So basically anyone who knows about it, just have to create an account with no special access and destroy your site.

Thanks to Wordfence team for responsibly disclosing this and then ensuring that it's patched for everyone. I am not associated with Wordfence in anyway :-)

Serghyo *
October 27, 2021
6:44 am

Hi, why is the severity of this authenticated vulnerability so high?

Ram Gall *
October 27, 2021
7:07 am

Hi Serghyo,
Complete deletion of all Database and Uploaded content results in a High impact to both Availability and Integrity, and there's not a lot of impact difference between authenticated vulnerabilities requiring low privileges vs unauthenticated vulnerabilities given that many WordPress sites, including nearly all e-commerce sites, allow open registration. This is according to the CVSS3.1 scoring model, which is admittedly imperfect for many situations such as XSS, but in this case I stand by the assessment as "losing everything on your site" is pretty high impact.