UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00217

HASHTHEMES BUG IN WORDPRESS ALLOWS SITE WIPE

DATE ISSUED: 1st November 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

The HashThemes Demo Importer plugin that is used to let administrators import demos for WordPress Themes contains a high-severity security flaw that allows subscribers to wipe a WordPress site, database content and uploaded media.

BREAKDOWN

Currently used in over 8,000 active installations on WordPress sites, this bug allows any authenticated users to completely wipe a WordPress site and associated databases with very little effort. Wordfence contacted WordPress following the disclosure process and went public with the information after receiving no response. That same day, WordPress pulled the plugin for HashThemes and added a patched version a few days later. The JavaScript-based technology Ajax in use with HashThemes allows new information to be fetched and presented on a page without the need to refresh failed to complete capability checks for many actions. The Ajax nonce was visible in the administration dashboard for all users of all privilege levels allowing anyone to completely reset all hosted content and databases with just one click.

REMEDIATION STEPS

- Install the patched version of the HashThemes plugin or update existing instances.
- Ensure backups are in place and working for all databases and content
- Ensure you have visibility over content management systems and servers as well as all plugins in order to effectively manage and maintain them. Ensure patches are applied where
- Check user access privilege settings on WordPress instances and use least-privilege, least-access and need-to-know as a guide.
- Check any plugins, templates, or add-ons are from reputable sources.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/wordpress-plugin-bug-wipe-sites/175826/