UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0284

CRITICAL WORDPRESS FLAW ALLOWS SITE TAKEOVER

DATE ISSUED: 27th February 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Threat actors are actively exploiting two critical-severity vulnerabilities in the Houzez theme and plugin for WordPress . Patchstack's researcher Dave Jong has discovered two critical flaws in the Houzez Theme and Plugin for WordPress that could allow the complete acquisition of a WordPress website.

BREAKDOWN

These premium add-ons are used mainly on real estate websites. WordPress is an open-source tool for website creation that supports hypertext preprocessor (PHP) language and is paired with a MySQL or MariaDB database with supported HTTPS. The first critical flaw, tracked as CVE-2023-26540, has a severity rating of 9.8. It could allow threat actors to bypass the authentication process and escalate privilege. The second critical security flaw tracked as CVE-2023-26009 has a severity rating of 9.8. An attacker could exploit these vulnerabilities by sending a request to the endpoint and listening to account creation requests. On the server side, a bug in the validation check allows the attacker to alter the request to create an administrator user on the site that could let an attacker take complete control of the WordPress site. This misconfiguration means an attacker would then be able to upload a backdoor to retain access and execute commands, injecting ads on the website, or redirecting traffic to other malicious sites. The vulnerabilities above impact the Houzez Theme Plugin version 2.7.1 and older and Houzez Login Register Plugin version 2.6.3 and older.

REMEDIATION STEPS

- Update and patch the to ensure the latest version of the software is running.
- Deploy network security solutions that can block attempted exploits and monitor network for Anomalous activity.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/critical-flaws-in-wordpress-houzez-theme-exploited-to-hijack-websites/