Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Shield Your Site: WordPress Houzez Theme and Plugin Flaws Uncovered

Date of Publication	Admiralty Code	TA Number
September 24, 2024	A1	TA2024368

Summary

First Seen: August 2024
Affected Products: WordPress Houzez theme and WordPress Houzez Login Register plugin
Impact: WordPress has released patches for two critical vulnerabilities in its Houzez theme and Houzez Login Register plugin, identified as CVE-2024-22303 and CVE-2024-21743. These vulnerabilities allow for privilege escalation, enabling malicious actors to elevate their access from low-privileged accounts to higher privileges, which poses a significant security risk. Users are strongly advised to update to the latest versions of the theme and plugin to safeguard their sites against potential exploitation.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-22303	WordPress Houzez Theme Privilege Escalation Vulnerability	WordPress Houzez Theme	✗	✗	✓
CVE-2024-21743	WordPress Houzez Login Register Plugin Privilege Escalation Vulnerability	WordPress Houzez Login Register Plugin	✗	✗	✓

Vulnerability Details

#1 WordPress has released critical patches addressing two significant vulnerabilities in its popular Houzez theme and the Houzez Login Register plugin, identified as CVE-2024-22303 and CVE-2024-21743. The Houzez theme is a widely utilized solution for real estate websites, offering an array of features tailored for real estate professionals, including advanced property listings, customizable search functionalities, and seamless integration with various real estate plugins. Its modern design and responsive layout have made it a favored choice for users looking to establish a robust online presence.

#2 The Houzez Login Register plugin complements the theme by enhancing user experience through custom login and registration forms, making it easier for users to create accounts and log into their websites. However, both the theme and the plugin have been found to contain vulnerabilities that can be exploited by malicious actors.

#3 CVE-2024-22303 affects the Houzez theme, while CVE-2024-21743 impacts the Houzez Login Register plugin. Both vulnerabilities allow attackers to elevate their privileges from a low-privileged user to an administrative level. If these flaws are exploited successfully, an attacker could take complete control of the affected website, posing severe risks to its security and integrity.

#4 The ability for attackers to gain elevated privileges is particularly concerning, as it opens the door for arbitrary actions that can severely compromise the website's functionality, data integrity, and user trust. Given the critical nature of these vulnerabilities, users are strongly urged to update their Houzez theme and Houzez Login Register plugin to the latest versions. This proactive step is essential to safeguard their websites from potential exploitation and maintain a secure online environment.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-22303	WordPress Houzez Theme Versions 3.2.4 and Prior	cpe:2.3:a:favethemes:houzez:*:*:*:*:*:*:*:*	CWE-266
CVE-2024-21743	WordPress Houzez Login Register Plugin Versions 3.2.5 and Prior	cpe:2.3:a:favethemes:houzez:*:*:*:*:*:*:*:*	CWE-266

Recommendations

Keep Plugins Updated: Ensure that all WordPress plugins, including WordPress Houzez Theme and the WordPress Houzez Login Register Plugin, are regularly updated to the latest versions to patch known vulnerabilities.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0004** Privilege Escalation	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation	

Patch Details

Update the WordPress Houzez theme and WordPress Houzez Login Register plugins to version 3.3.0.

References

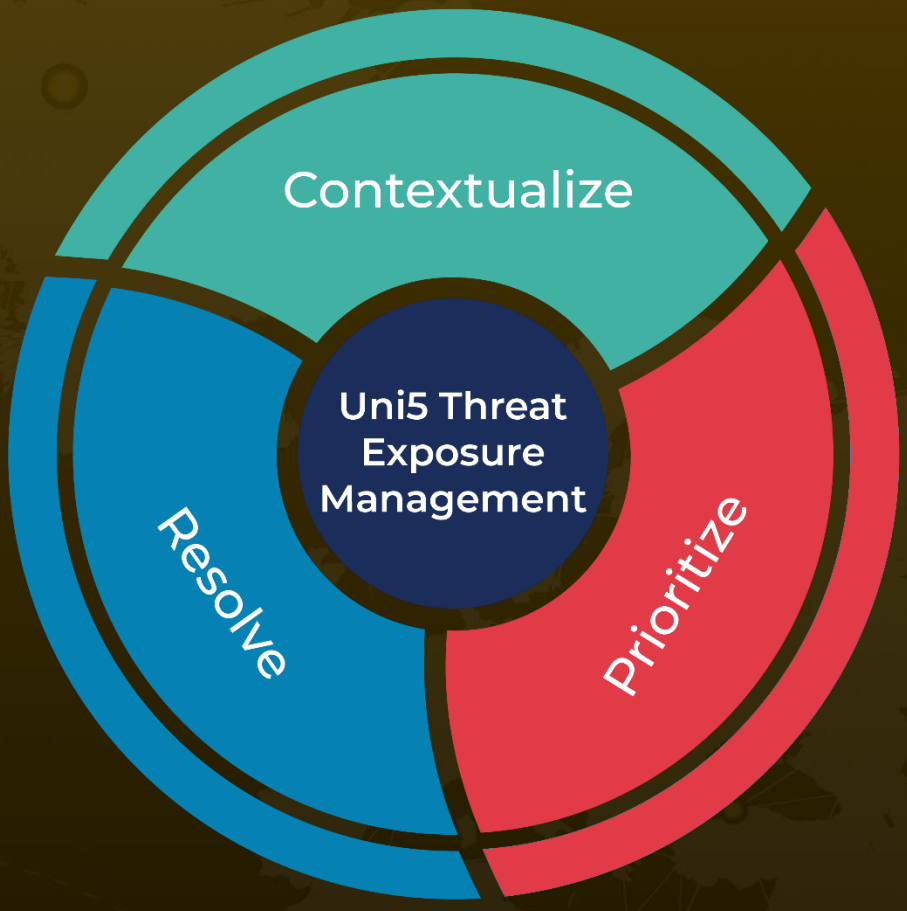
https://patchstack.com/database/vulnerability/houzez/wordpress-houzez-theme-3-2-4-privilege-escalation-vulnerability?_s_id=cve

https://patchstack.com/database/vulnerability/houzez-login-register/wordpress-houzez-login-register-plugin-3-2-5-privilege-escalation-vulnerability?_s_id=cve

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 24, 2024 • 6:40 AM

More at www.hivepro.com