AL2025_02 Critical Zero-Day Vulnerabilities Impact WordPress Real Estate Plugins (23rd January 2025)

Description

Two critical zero-day vulnerabilities have been discovered in WordPress products widely used in real estate websites: the RealHome theme and the Easy Real Estate plugin. These vulnerabilities allow unauthenticated attackers to escalate their privileges to administrative levels, granting them full control of the affected WordPress websites. The flaws, tracked as CVE-2024-32444 (RealHome) and CVE-2024-32555 (Easy Real Estate), were first identified by researchers at Patchstack in September 2024. Despite multiple efforts to contact the vendor, InspiryThemes, no security fixes have been implemented in subsequent updates. The issues remain unpatched and exploitable, posing a serious threat to thousands of websites. The RealHome theme alone is estimated to be active on over 32,600 websites, making this vulnerability a significant risk for site owners and their visitors.

Attack Details

Attackers exploit iMessage's built-in phishing protection by persuading users to reply to messages from unknown senders. These messages, often disguised as urgent notifications from reputable entities such as shipping companies or government agencies, claim issues like unpaid tolls or delivery problems. They instruct recipients to reply with specific keywords, such as "Y," which re-enables disabled links and bypasses Apple's protections. By manipulating human behavior leveraging familiarity with responses like "Yes" or "No", attackers increase the likelihood of user compliance. Once a user replies, they not only enable potentially malicious links but also signal that they are an active target, opening the door to follow-up attacks.

Remediation

Since there are no security patches to address these vulnerabilities, website owners must take immediate steps to mitigate the risk:

- **Disable the RealHome Theme and Easy Real Estate Plugin**
- **Restrict User Registration:** Disable user registration on the affected websites to prevent attackers from exploiting the inspiry_ajax_register function.
- **Restrict Admin Email Exposure:** Ensure administrative email addresses are not publicly visible to reduce the risk of exploitation via the social login flaw.
- **Monitor for Exploitation Attempts:** Implement a Web Application Firewall (WAF) to block suspicious requests. Regularly monitor logs for abnormal activity or signs of exploitation.
- **Backup Data:** Ensure you have up-to-date backups of your website and database in case of a successful attack.

- **Stay Updated:** Regularly check for updates or advisories from InspiryThemes and security organizations like Patchstack. Subscribe to notifications about vulnerabilities in WordPress themes and plugins you use.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

1. Toulas, B. (2025, January 22). Critical zero-days impact premium WordPress real estate plugins. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/critical-zero-days-impact-premium-wordpress-real-estate-plugins/
2. Writer, S. (2025, January 23). WordPress Real-Estate plugin vulnerability exposes 32k+ websites. Retrieved from Top Tech. https://toptechgh.com/wordpress-real-estate-plugin-vulnerability-exposes-websites/