AL2025_28 OttoKit WordPress Plugin Auth Bypass Vulnerability Exploited Within Hours (June 11, 2025)

Description

A high-severity authentication bypass vulnerability (CVE-2025-3102) in the OttoKit WordPress plugin (formerly known as SureTriggers) has come under active exploitation mere hours after public disclosure. The OttoKit plugin, which allows seamless automation across plugins and external tools like WooCommerce, Mailchimp, and Google Sheets, is currently installed on over 100,000 websites. The vulnerability affects all versions of the plugin up to 1.0.78, allowing attackers to bypass authentication and gain administrative privileges. The vendor released a patched version, 1.0.79, on April 3, 2025. Site owners are urged to upgrade immediately.

Attack Details

The vulnerability identified as **CVE-2025-3102** affects the **OttoKit plugin** (formerly SureTriggers) in versions 1.0.78, with a patch issued in version 1.0.79. Disclosed on April 9, 2025, the flaw was actively exploited within just four hours. It stems from a missing check for empty values in the authenticate_user() function, which handles REST API authentication. If the plugin is not configured with an API key, the secret_key remains empty, allowing attackers to bypass authentication by sending a REST API request with an empty st_authorization header. This can lead to severe consequences including the creation of unauthorized administrator accounts, full site takeover, manipulation of site content and settings, installation of malicious plugins or themes, and exfiltration or destruction of data.

Remediation

Immediate Plugin Update:

- Upgrade to OttoKit version 1.0.79 or later via the WordPress admin panel or manually via FTP.

Audit and Cleanup:

- Check for unknown admin or user accounts and remove any unauthorized entries.
- Examine recently added or modified plugins/themes.
- Review server and plugin logs for REST API misuse or anomalies.

Hardening Measures:

- Enforce strong API key usage in the OttoKit plugin configuration.
- Restrict REST API access using a Web Application Firewall (WAF).
- Monitor with security plugins like Wordfence or Sucuri for early warning signs.

Report and Communicate:

- Notify your team or stakeholders of the issue and any actions taken.
- Consider informing users if data integrity or privacy may have been affected.

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

References

- The Hacker News. (n.d.). OttoKit WordPress plugin Admin creation vulnerability under active exploitation. Retrieved from https://thehackernews.com/2025/04/ottokit-wordpress-plugin-admin-creation.html
- Toulas, B. (2025, April 10). Hackers exploit WordPress plugin auth bypass hours after disclosure. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-exploit-wordpress-plugin-auth-bypass-hours-after-disclosure/