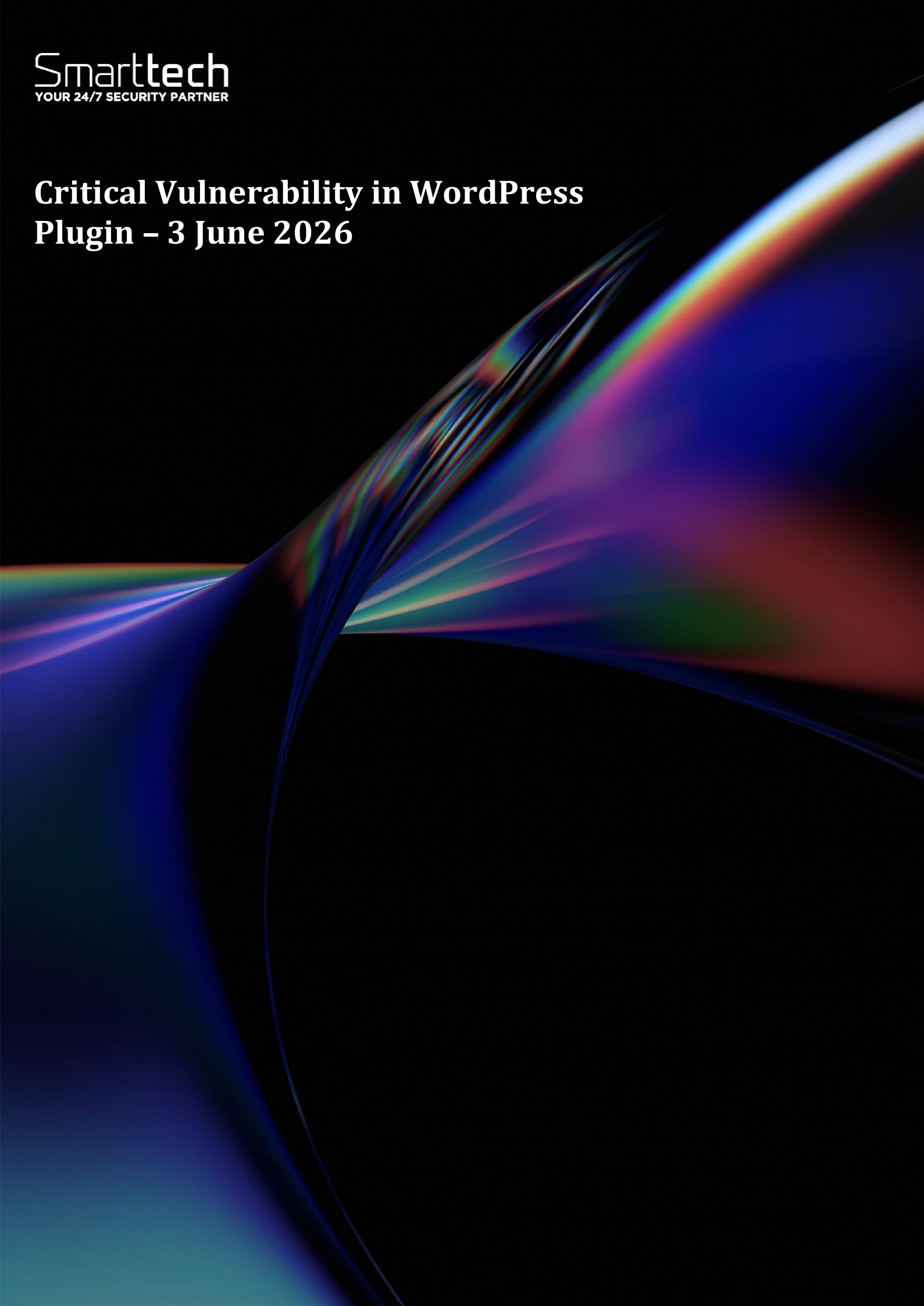
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Vulnerability in WordPress Plugin – 3 June 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	85
Authors	Ana-Maria Nastase < ana.nastase@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-06-02
Issue Date	2026-06-03

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

A critical vulnerability was discovered in the Kirki WordPress plugin that allows unauthenticated attackers to take over arbitrary user accounts, including administrator accounts, through a flaw in the password reset mechanism. Successful exploitation could lead to full site compromise, enabling attackers to gain administrative access, modify website content, install malicious plugins or backdoors, and maintain persistent control over the affected WordPress site.

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Affected Versions

6.0.0 - 6.0.6

Patched Version

6.0.7

TECHNICAL SUMMARY

Kirki is a plugin that provides freeform page building, website building, and WordPress Customizer enhancements. As part of its frontend account management features, the plugin exposes a custom REST API endpoint that handles password reset requests. This plugin is installed on over 500,000 WordPress sites, with approximately 150,000 currently running vulnerable versions.

The issue originates from the **handle_forgot_password()** function in the **CompLibFormHandler** class, where the custom REST API endpoint for password resets accepts an attacker-supplied email address instead of using the account's registered email.

By sending a crafted password reset request containing a target username and an attacker-controlled email, attackers can receive the reset link and gain full administrative access, potentially installing malicious plugins, injecting web shells, or exfiltrating sensitive data. No authentication is required to exploit this issue.

The assigned CVE ID is **CVE-2026-8206** with a **CVSS Score** of **9.8**

Potential Impact

Successful exploitation could allow attackers to gain full administrative control over WordPress sites, install backdoors and web shells, and exfiltrate user data and site content, leading to service disruption, data exposure, or full infrastructure compromise.

Recommendations

Smarttech247 team **highly** recommends the following actions be taken:

1. Upgrade the Kirki plugin to version 6.0.7 or later immediately, as this vulnerability has been fully addressed in the patched release.
2. Review user accounts and privilege assignments for any unauthorized accounts, suspicious password resets, or unexpected permission changes.
3. Audit website files, plugins, and themes for unauthorized modifications, malicious uploads, web shells, or other indicators of compromise.
4. Deploy and maintain Web Application Firewall (WAF) protections to detect and block malicious requests targeting the vulnerable password reset REST API endpoint.
5. Ensure WordPress plugins, themes, and core installations are updated in a timely manner to reduce exposure to known vulnerabilities and prevent exploitation.
6. Apply the Principle of Least Privilege to all user accounts, services, and administrative functions to minimize the impact of potential compromise.
7. Consider implementing virtual patching solutions, such as firewall rules or managed security services, to provide interim protection when immediate patch deployment is not possible.
8. Monitor security alerts and logs for indicators of attempted exploitation and verify that security controls, including firewall protections, are functioning as expected.

References

https://www.wordfence.com/blog/2026/06/unauthenticated-privilege-escalation-vulnerability-patched-in-kirki-wordpress-plugin/
https://orca.security/resources/blog/kirki-wordpress-plugin-vulnerability-cve-2026-8206/
https://www.cve.org/CVERecord?id=CVE-2026-8206

CVE

CVE-2026-8206

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com