

Alert Bulletin

Bulletin N.: 103

Publication Date: 19/09/2026

Subject: Alert 2026-103 Click2Shell in WordPress allows forced theme installation and can be chained to RCE

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions	Fixed version
WordPress Core	WordPress 6.0 up to versions prior to the corresponding security patch	WordPress 7.1.1 or equivalent security update for the supported branch
WordPress Core — older branches with security support	Supported versions since WordPress 4.7 affected by the issue	Maintenance/security update published on September 17, 2026

* WordPress confirmed that the issue is present from version **6.0** up to versions immediately preceding the fix. The security update of September 17, 2026 includes fixes for supported branches since WordPress 4.7

Description

A vulnerability was identified in the WordPress core that allows a specially crafted URL to force the installation and preview of a legitimate theme from the WordPress.org repository when an authenticated administrator opens the link. The vulnerability, named **Click2Shell**, was fixed in **WordPress 7.1.1** and in the equivalent updates for supported branches. There is no CVE published yet, but a score of 9.6 (critical) is estimated.

Click2Shell is a URL-induced forced theme installation vulnerability. The issue occurs because two WordPress components interpret a parameter included in a manipulated URL differently: the WordPress.org repository interprets it as the normal name of a valid theme, while the administrator's browser reuses the original content—including additional characters—within JavaScript code used to locate an element on the page.

The use of specially prepared characters allows the browser selector to point to the **Install** button and the WordPress script itself to execute the installation action. Since the administrator already has an active session, the browser automatically includes their permissions and security token (*nonce*), so the attacker does not need to know credentials or obtain that token.

Click2Shell should not be confused with **wp2shell**, another WordPress Core vulnerability disclosed in July 2026. wp2shell does not require login or user interaction, and CISA included it as an actively exploited vulnerability; Click2Shell, on the other hand, requires an authenticated administrator to open a specially crafted link and has no known active exploitation.

Solution

The official solution is to update WordPress to **7.1.1** or to the security update published for the corresponding supported branch. The update can be performed from the administration panel at **Dashboard > Updates > Update Now**, or via the installation package available from WordPress.org.

There is no standalone *workaround* that eliminates the URL interpretation flaw. Disabling themes, restricting the administration panel, and avoiding suspicious links are temporary controls that reduce the likelihood of exploitation, but they do not replace applying the patch.

After updating, it is recommended to keep only necessary themes and plugins, apply security updates promptly, and use additional controls to protect administrative sessions.

Additional information:

- <https://wordpress.org/news/2026/09/wordpress-7-1-1-maintenance-and-security-release/>
- <https://wordpress.org/documentation/wordpress-version/version-7-1-1/>
- <https://thehackernews.com/2026/09/new-wordpress-click2shell-flaw-forces.html>