Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Unpatched Flaw Found in TI WooCommerce Wishlist Plugin

Date of Publication	Admiralty Code	TA Number
May 30, 2025	A1	TA2025169

Summary

First Seen: March 26, 2025
Affected Product: TemplateInvaders TI WooCommerce Wishlist Plugin
Affected Platform: WordPress
Impact: CVE-2025-47577 is a critical vulnerability in the TI WooCommerce Wishlist plugin for WordPress (≤2.9.2) that allows unauthenticated attackers to upload malicious files and gain full server control. The flaw arises from disabled file validation in the plugin's upload function, triggered only when the WC Fields Factory plugin integration is enabled. Over 100,000 active sites are at risk, making prompt action essential. No official patch is available yet, so site owners should disable the plugin and apply security measures immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-47577	TemplateInvaders TI WooCommerce Wishlist Plugin Unrestricted File Type Upload Vulnerability	TemplateInvaders TI WooCommerce Wishlist Plugin	⊗	⊗	⊗

Vulnerability Details

#1

CVE-2025-47577 is a critical vulnerability discovered in the TemplateInvaders TI WooCommerce Wishlist plugin for WordPress, affecting all versions up to and including 2.9.2. With over 100,000 active installations, this plugin allows online store customers to save and share product wishlists. The flaw enables unauthenticated attackers to upload arbitrary files, including malicious web shells, directly to the server, bypassing WordPress's standard file validation mechanisms. This can lead to full server compromise, remote code execution, and total site takeover.

#2

The vulnerability stems from a misconfiguration in the plugin's tinvwl_upload_file_wc_fields_factory function, which utilizes WordPress's wp_handle_upload() without proper safeguards. Specifically, the parameters test_form and test_type are set to false, disabling essential checks for form origin and MIME type. This insecure implementation allows attackers to upload executable files without needing authentication or user interaction. Notably, this upload functionality is only reachable when the WC Fields Factory plugin is also installed and its integration is enabled, an important prerequisite that slightly narrows the attack vector.

#3

The vulnerability was publicly disclosed in May 2025 after being initially reported in March. As of late May 2025, no official patch has been released by the plugin developer. Currently, there is no publicly available proof-of-concept exploit or confirmed evidence of widespread exploitation. However, the ease of execution, lack of authentication requirement, and severity of impact make this a high-priority vulnerability. Site administrators using this plugin are strongly urged to take immediate action and monitor for official updates.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-47577	TemplateInvaders TI WooCommerce Wishlist Plugin versions upto 2.9.2	cpe:2.3:a:templateinvaders:ti_woocommerce_wishlist_plugin:*:*:*:*:*:*:*:*	CWE-434

Recommendations

Deactivate and Remove the Plugin: Immediately deactivate and uninstall the TI WooCommerce Wishlist plugin, especially if the WC Fields Factory plugin is also installed and integrated. This action eliminates the vulnerable code path, preventing potential exploitation.

Alternative Plugin: Consider switching to a reputable alternative wishlist plugin, such as YITH WooCommerce Wishlist, WPC Smart Wishlist for WooCommerce, or WooCommerce Wishlists, to maintain functionality while ensuring better security.

Implement a Web Application Firewall (WAF): Deploy a WAF solution like Wordfence, Patchstack, or Cloudflare to monitor and block malicious file upload attempts. Ensure the WAF is configured to inspect and filter HTTP POST requests targeting file upload endpoints.

Enforce Strict File Upload Policies: Restrict file uploads to specific, necessary file types (e.g., images: .jpg, .png) and validate MIME types server-side. Implement server-side checks to reject files with executable extensions such as .php, .exe, or .sh.

Audit and Harden Server Permissions: Review and adjust file system permissions to ensure that upload directories (e.g., /wp-content/uploads/) do not have execute permissions. Set appropriate ownership and permissions to limit the ability to execute uploaded files.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0042 Resource Development	TA0001 Initial Access	TA0040 Impact
TA0002 Execution	T1190 Exploit Public-Facing Application	T1588 Obtain Capabilities	T1588.005 Exploits
T1588.006 Vulnerabilities	T1505.003 Web Shell	T1505 Server Software Component	T1059 Command and Scripting Interpreter
T1485 Data Destruction	T1608.001 Upload Malware	T1608 Stage Capabilities	

Patch Details

No official patch is available yet, but a future fix is expected to restore proper file validation and restrict upload access to authenticated users.

Link:
https://wordpress.org/plugins/ti-woocommerce-wishlist/

References

https://patchstack.com/articles/unpatched-critical-vulnerability-in-ti-woocommerce-wishlist-plugin/

https://patchstack.com/database/wordpress/plugin/ti-woocommerce-wishlist/vulnerability/wordpress-ti-woocommerce-wishlist-2-9-2-arbitrary-file-upload-vulnerability

https://x.com/rxerium/status/1928033483588239619

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.

Contextualize
Prioritize
Resolve
Uni5 Threat Exposure Management

REPORT GENERATED ON

May 30, 2025 • 7:30 AM

More at www.hivepro.com