

**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

4 September 2026

**Advisory 256: YITH Request a Quote for WooCommerce Premium
Unauthenticated Broken Access Control (CVE-2026-84238).**

Release Date: 3rd September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and e-commerce teams that operate a WooCommerce-based WordPress store using the YITH Request a Quote for WooCommerce Premium extension. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-84238 is a critical, unauthenticated broken access control vulnerability in YITH Request a Quote for WooCommerce Premium, a paid extension by YITH (Your Inspiration Themes) - an established WooCommerce extension vendor whose free companion plugin alone has 10,000+ active installations on WordPress.org that lets store owners hide prices and "Add to cart" buttons and instead let customers request custom quotes.

What are the systems affected?

The following version(s) are affected:

- YITH Request a Quote for WooCommerce Premium before 4.46.0 - (Affected)

YITH Request a Quote for WooCommerce Premium 4.46.0 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Directly access the unprotected functionality**
 - An unauthenticated attacker sends a request directly to the plugin functionality that is missing its required authorization check, without needing to log in or hold any account on the WooCommerce store.
2. **Read, modify, or disrupt data the check was meant to protect**
 - Because the plugin does not verify that the caller is permitted to invoke this functionality, the attacker can carry out the action it was meant to restrict — potentially including access to quote-request data submitted by customers, or interference with the store's quote-management workflow, depending on the specific functionality reached.

Attack vectors:

- A network-based, unauthenticated request against any internet-reachable WooCommerce store running an affected version of YITH Request a Quote for WooCommerce Premium.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but the vulnerability requires no authentication at all, which typically shortens the window before opportunistic scanning begins.

Successful exploitation may allow attackers to:

- Access or manipulate quote-request data and related store functionality that should have been restricted to authorized users, without ever holding a legitimate credential.
- Disrupt the affected store's quote-request workflow, and depending on the specific data exposed, potentially obtain customer-submitted information collected through the quote-request process.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update YITH Request a Quote for WooCommerce Premium to version 4.46.0 or later through the WordPress admin dashboard (Plugins > Installed Plugins), where this vulnerability is fixed.

2. Treat this as urgent given the unauthenticated, no-privilege-required nature of the flaw

3. Audit the estate for YITH Request a Quote installations

4. Consider a Web Application Firewall (WAF) as an interim layer of defence

5. Review quote-request data and access logs for suspicious activity

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-84238>
2. <https://yithemes.com/themes/plugins/yith-woocommerce-request-a-quote/>