CVE-2025-26776

WORDPRESS CHATY PRO

PLUGIN ARBITRARY FILE

Vairav CVE Report

Date: March 06, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Patchstack OÜ has disclosed a critical vulnerability (CVE-2025-26776) in the WordPress Chaty Pro plugin that allows unauthenticated attackers to upload arbitrary files, including web shells, to vulnerable servers. This flaw enables remote code execution (RCE), potentially leading to full system compromise. Organizations using affected versions should take immediate remediation actions.

VULNERABILITY DETAILS

CVE-2025-26776: WordPress Chaty Pro Plugin Arbitrary File Upload

Description: This vulnerability stems from improper file upload validation, allowing attackers to upload malicious files to a vulnerable WordPress server. Exploiting this flaw can lead to remote code execution, data theft, and full system takeover.

Impact: Unauthorized file uploads, potential web shell execution, and full site compromise.

CVSS Score: 10.0 (Critical)

AFFECTED VERSIONS

Chaty Pro plugin versions up to and including 3.3.3.

- *Fixed in version 3.3.4*

EXPLOIT DETAILS

- Attackers can exploit this vulnerability remotely without authentication.
- A crafted malicious file uploaded via the plugin can lead to arbitrary code execution on the server.
- This can result in complete control over the affected WordPress site and its underlying hosting environment

RECOMMENDED ACTIONS

- Upgrade to Chaty Pro version 3.3.4 immediately to mitigate this vulnerability.

For Users Unable to Upgrade:

- Disable file upload functionality in WordPress where possible.
- Restrict write permissions on server directories handling user-uploaded files.
- Use security plugins to monitor and block suspicious file uploads.

ADDITIONAL SECURITY MEASURES

- Limit admin privileges to trusted users only.
- Deploy a WAF to block malicious file uploads.
- Conduct frequent vulnerability assessments of plugins and themes.

REFERENCES

https://securityonline.info/cve-2025-26776-cvss-10-in-chaty-pro-plugin-exposes-thousands-of-wordpress-sites-to-takeover/

https://www.cve.org/CVERecord?id=CVE-2025-26776

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com