Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

WordPress Plugin Bug CVE-2025-11833 Hands Hackers the Admin Throne

Date of Publication	Admiralty Code	TA Number
November 7, 2025	A1	TA2025338

Summary

First Seen: October 11, 2025
Affected Products: WordPress Plugin Post SMTP
Impact: A critical vulnerability, CVE-2025-11833, in the Post SMTP WordPress plugin installed on over 400,000 websites allows unauthenticated attackers to gain full administrative control by exploiting a missing capability check. Affecting all versions up to 3.6.0, the flaw enables access to logged emails, including password reset messages, allowing attackers to reset administrator passwords and hijack entire sites. Attackers have already begun targeting this vulnerability, with over 4,500 attacks reportedly blocked so far.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-11833	WordPress Plugin Post SMTP Missing Authorization Vulnerability	WordPress Plugin Post SMTP	✗	✗	✓

Vulnerability Details

#1 Post SMTP, a WordPress plugin used to replace the default PHP mail function with an SMTP mailer, contains a critical vulnerability tracked as CVE-2025-11833 that affects all versions up to and including 3.6.0. The Post SMTP has a missing capability check in its __construct function, which permits unauthorized access to sensitive log data.

#2 An unauthenticated attacker can exploit this flaw to read arbitrary logged emails stored by the plugin, including password reset messages and their links. By triggering a password reset for an administrator account and retrieving the corresponding reset email from the logs, the attacker can change that user's password and gain administrative control of the site.

#3 The scope of impact extends beyond individual account compromise. The vulnerability affects a substantial portion of the WordPress ecosystem, with over 400,000 active installations at risk.

#4 With administrative access, the attacker can perform any action available to a legitimate administrator, like upload and activate plugins or themes, including malicious ZIPs that install backdoors, modify posts and pages, and redirect site visitors to other malicious destinations. The vulnerability, therefore, enables complete account and site takeover.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-11833	Post SMTP WordPress Plugin Affected all versions up to, and including 3.6.0	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*	CWE-862

Recommendations

Immediate Patch Deployment: Update the Post SMTP plugin immediately to version 3.6.1 or later, released on October 29, 2025, which includes proper authorization checks. Audit all WordPress user accounts and password reset logs for any signs of unauthorized access that may have occurred between installation and patching. If the vulnerable version was publicly accessible, enforce password resets for all administrative accounts. Additionally, review any site modifications made during the vulnerability window to identify and remove potential malicious changes.

Strengthening Defensive Controls: Implement Web Application Firewall (WAF) rules to block unauthorized access to REST API endpoints and enhance overall request filtering. Enable multi-factor authentication (MFA) for all WordPress administrative accounts to reduce the risk of credential-based compromise. Apply network segmentation to restrict access to WordPress admin interfaces and minimize exposure to external threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0009 Collection	TA0007 Discovery	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1098 Account Manipulation	T1059 Command and Scripting Interpreter	T1005 Data from Local System	T1114 Email Collection
T1040 Network Sniffing			

Patch Link

https://wordpress.org/plugins/post-smtp/#developers

References

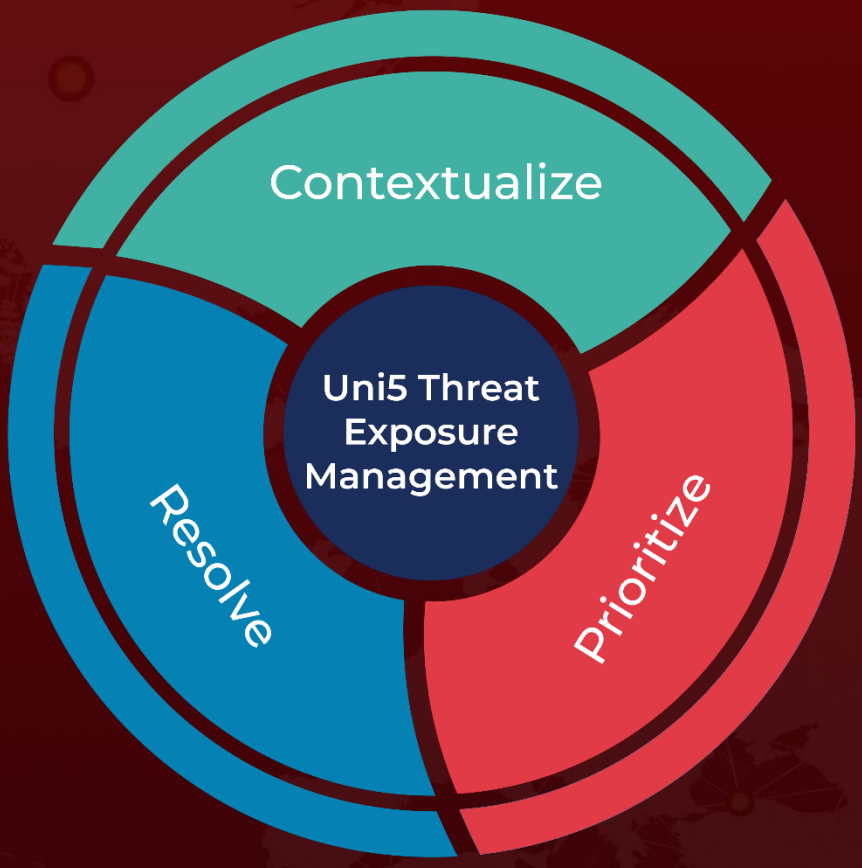
https://www.wordfence.com/blog/2025/11/400000-wordpress-sites-affected-by-account-takeover-vulnerability-in-post-smtp-wordpress-plugin/

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/post-smtp/post-smtp-complete-smtp-solution-with-logs-alerts-backup-smtp-mobile-app-360-missing-authorization-to-account-takeover-via-unauthenticated-email-log-disclosure

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.



REPORT GENERATED ON

November 7, 2025 • 01:30 AM

More at www.hivepro.com