Silent Breach Discovers Critical WordPress Plugin Vulnerability

Our research team has recently discovered a critical vulnerability affecting the WP Test Email WordPress plugin, now tracked as CVE-2025-2325.

NYC, NY, UNITED STATES, March 18, 2025 /EINPresswire.com/ -- At Silent Breach, our labs work at the forefront of cybersecurity research, identifying vulnerabilities before they can be exploited by attackers.

Our research team has recently discovered a critical vulnerability affecting the WP Test Email WordPress plugin, now tracked as CVE-2025-2325. Upon discovering this vulnerability, our team followed the appropriate disclosure practices, notifying the plugin developers to ensure a timely patch was released. As of now, WP Test Email version 1.1.9 has been released, addressing the issue.

Snapshot
Name: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

CVE: CVE-2025-2325

CVSS: 7.2 (High)

Software Type: Plugin

Software Slug: wp-test-email (view on wordpress.org)

Patched? Yes

Remediation: Update to version 1.1.9, or a newer patched version

Affected Version: All versions up to and including 1.1.8

Patched Version: 1.1.9

Vulnerability Overview

CVE-2025-2325 is an Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability found in WP Test Email v1.1.8. This plugin, used by WordPress administrators to test email functionality, exposes websites to potential attacks by allowing malicious scripts to be injected and executed within the administrator's browser.

This vulnerability is particularly dangerous because it does not require authentication to exploit. An attacker can inject malicious JavaScript code that will execute when an administrator accesses the affected page. This can lead to:

Session Hijacking: Attackers can steal session cookies, potentially taking over admin accounts.

Defacement & Content Manipulation: Unauthorized modifications to the website's appearance or content.

Phishing Attacks: Redirecting admins to fake login pages to harvest credentials.

Malware Injection: Delivering further payloads to compromise the system.

Recommendations

If your website is running WP Test Email v1.1.8 or earlier, we strongly recommend taking the following actions:

Update Immediately: Ensure your plugin is updated to version 1.1.9 or higher.

Review Admin Logs: Look for any unusual activity that might indicate an attempted exploit.

Enhance Security Posture: Implement a Web Application Firewall (WAF) and enforce Content Security Policies (CSP) to mitigate similar threats in the future.

Conclusion

Silent Breach remains committed to securing the digital landscape by identifying and responsibly disclosing vulnerabilities before they can be leveraged by cybercriminals. We commend the WordPress security community for their swift response in addressing this issue.

For further details on CVE-2025-2325, visit the official Wordfence advisory here.

Silent Breach provides specialized services to help organizations identify and address

vulnerabilities like CVE-2025-2325. Our penetration testing teams simulate sophisticated attacks to identify weaknesses, while our SOC monitoring solutions enable continuous threat detection and rapid incident response. For organizations navigating compliance requirements, our expertise ensures alignment with standards such as ISO 27001 and SOC 2.

For more information on how your organization may be impacted by CVE-2025-2325 or for additional guidance, please contact Silent Breach at contact@silentbreach.com.

About Silent Breach: Silent Breach is an award-winning provider of cyber security services. Our global team provides cutting-edge insights and expertise across the Data Center, Enterprise, SME, Retail, Government, Finance, Education, Automotive, Hospitality, Healthcare and IoT industries.

Daniel Rhodes
Silent Breach
+1 727-497-7941
email us here