10 years CERT-EU

Security Advisory 2024-011

Vulnerability in Wordpress POST SMTP Mailer Plugin

January 19, 2024 — v1.0

TLP:CLEAR

History:

- *19/01/2024 — v1.0 – Initial publication*

Summary

On January 10, 2024, an authorisation bypass vulnerability has been discovered in the "*POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP*" plugin for WordPress. This vulnerability, identified as `CVE-2023-6875` (CVSS score of 9.8)[1], may allow an unauthenticated attacker to reset the API key used to authenticate to the mailer and view logs, including password reset emails on WordPress sites that use this plugin [2].

This vulnerability could affect sites that have the POST SMTP Mailer plugin installed and configured, which is estimated to be over 300,000 sites [3].

Technical Details

The POST SMTP Mailer plugin for WordPress is vulnerable to unauthorised access of data and modification of data due to a type juggling issue on the connect-app REST endpoint in all versions up to, and including, 2.8.7. This makes it possible for unauthenticated attackers to reset the API key used to authenticate to the mailer and view logs, including password reset emails, allowing website takeover.

Affected Products

"*POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP*" Wordpress plugin version 2.8.7 and below.

Recommendations

To mitigate this vulnerability, update the vulnerable plugin to at least version 2.8.8 as it contains the necessary fixes.

It is also advised to monitor their WordPress sites for any signs of unauthorised changes, such as injected scripts or deleted directories.

References

[1] https://www.cve.org/CVERecord?id=CVE-2023-6875

[2] https://www.wordfence.com/blog/2024/01/type-juggling-leads-to-two-vulnerabilities-in-post-smtp-mailer-wordpress-plugin/

[3] https://wordpress.org/plugins/post-smtp/