مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in FluentSMTP Plugin

Tracking #:432316554

Date:25-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a severe vulnerability has been discovered in the FluentSMTP plugin, which is used by over 300,000 WordPress websites to enhance email deliverability.

TECHNICAL DETAILS:

A severe vulnerability, tracked as CVE-2024-9511, has been discovered in the FluentSMTP plugin, which is used by over 300,000 WordPress websites to enhance email deliverability. The vulnerability has been assigned a CVSS score of 9.8, indicating its critical severity. This flaw allows unauthenticated attackers to execute arbitrary code on vulnerable websites, potentially leading to website compromise, data breaches, and full server takeover.

Vulnerability Details:

- **CVE-2024-9511**
- CVSS Score: 9.8 (Critical)
- Potential Impact: The vulnerability allows unauthenticated attackers to inject arbitrary PHP objects.
- Exploitability: While the vulnerability itself doesn't have a specific POP (Privilege Escalation) chain in FluentSMTP, if a system has other vulnerable plugins or themes that provide a POP chain, it could lead to:
  - Deletion of arbitrary files on the server.
  - Retrieval of sensitive information.
  - Execution of arbitrary code, potentially giving attackers full control over the WordPress site or the server.

Affected Versions: <= 2.2.82

Fixed Versions:2.2.83, or a newer patched version

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update FluentSMTP to the latest version at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-9511