مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Gravity SMTP plugin

Tracking #:432319177

Date:22-06-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in the Gravity SMTP WordPress plugin is being actively exploited. The flaw allows unauthenticated attackers to access sensitive system information, API keys, OAuth tokens, and email service credentials through an exposed REST API endpoint.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-4020 – Information Disclosure Vulnerability**
- **Severity:** Medium | **CVSS:** 5.3
- A flaw in the Gravity SMTP REST API endpoint (/wp-json/gravitysmtp/v1/tests/mock-data) allows unauthenticated users to access sensitive information due to improper access controls. By appending the query parameter ?page=gravitysmtp-settings, attackers can retrieve a detailed system report containing sensitive configuration data.
- Exposed information may include WordPress configuration details, plugin and theme information, database details, and API credentials for services such as Amazon SES, Google, Mailjet, Resend, and Zoho.
- Successful exploitation could allow attackers to abuse email services, harvest credentials, and gather intelligence for further compromise of affected environments.

Affected Versions

- Gravity SMTP WordPress Plugin Versions prior to 2.1.5

Fixed Version

- Gravity SMTP version 2.1.5 or later.

Indicators of Compromise (IoCs)

IP Addresses:

- 45[.]148[.]10[.]95
- 193[.]32[.]162[.]60
- 176[.]65[.]148[.]139
- 173[.]199[.]90[.]188
- 45[.]148[.]10[.]120
- 185[.]8[.]107[.]155
- 185[.]8[.]106[.]37
- 185[.]8[.]106[.]92
- 185[.]8[.]106[.]145
- 176[.]65[.]148[.]30

Suspicious Request:

GET /wp-json/gravitysmtp/v1/tests/mock-data?page=gravitysmtp-settings

RECOMMENDATIONS:

- Apply the latest security updates and patches to affected systems.
- Review logs for signs of suspicious or unauthorized activity.
- Reset and rotate potentially exposed credentials, API keys, and access tokens.

- Monitor systems and network traffic for indicators of compromise.
- Restrict access to sensitive services and administrative interfaces where possible.
- Implement security monitoring and alerting to detect potential exploitation attempts.
- Maintain regular backups and ensure incident response procedures are up to date.

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://www.wordfence.com/blog/2026/06/attackers-actively-exploiting-sensitive-information-exposure-vulnerability-in-gravity-smtp-plugin/