Gravity SMTP WordPress Plugin Information Disclosure Vulnerability

Severity Level: Medium

Components Affected

- Gravity SMTP WordPress Plugin versions prior to 2.1.5

Overview

A vulnerability has been identified in the Gravity SMTP WordPress plugin. An unauthenticated attacker could exploit this vulnerability to access sensitive information, including API keys, OAuth tokens, configuration details, and system information. Successful exploitation may facilitate unauthorized access to third-party email services and provide valuable reconnaissance data for subsequent attacks against the affected environment.

Description

A security vulnerability has been discovered in the Gravity SMTP WordPress plugin, affecting approximately 100,000 installations. The vulnerability is tracked as CVE-2026-4020 and has been assigned a CVSS score of 5.3.

The vulnerability exists because the Gravity SMTP plugin exposes a REST API endpoint located at ***/wp-json/gravitysmtp/v1/tests/mock-data*** that is accessible without authentication due to an improperly configured permission callback. By appending the ***?page=gravitysmtp-settings*** query parameter to the request, an unauthenticated attacker can trigger the plugin to generate and return a detailed system report containing sensitive information, including configuration details, API keys, OAuth tokens, WordPress environment information, server details, and other data that could be leveraged for unauthorized access, credential abuse, or further attacks against the affected website.

An unauthenticated attacker may obtain the following information:

- PHP Version
- Loaded PHP extensions
- Web server versions
- Document root path
- Database server type and version
- WordPress version

- Active plugins and versions
- Active WordPress theme
- WordPress configuration details
- Database table names
- API keys/tokens configured in the plugin, such as Amazon SES, Google, Mailjet, Resend, and Zoho

Impact

- Information Disclosure
- Exposure of API Keys and OAuth Tokens
- Unauthorized Use of Third-Party Email Services
- Credential Harvesting
- Reconnaissance for Follow-on Attacks
- Potential Service Abuse
- Increased Risk of Targeted Exploitation

Solution/ Workarounds

Before installation of the software, please visit the vendor web-site for more details.

Apply fixes issued by the vendor:

- Upgrade Gravity SMTP to version 2.1.5 or later.
- Rotate all exposed API keys, OAuth tokens, and credentials associated with email integrations after updating.
- Review server logs for suspicious requests to the particular endpoint.
- Investigate any evidence of unauthorized access or credential abuse.

Reference

- https://thehackernews.com/2026/06/hackers-exploit-gravity-smtp-wordpress.html
- https://securityboulevard.com/2026/06/hackers-exploit-gravity-smtp-wordpress-plugin-vulnerability/

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.