The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/25/2019

SUBJECT:
A Vulnerability in WordPress Easy WP SMTP Plugin Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in the WordPress Easy WP SMTP Plugin that could allow for remote code execution. WordPress is a web-based publishing application implemented in PHP, and the Easy WP SMTP Plugin allows website administrators to configure an SMTP server for outgoing emails. Successful exploitation of this vulnerability could allow for remote code execution with elevated privileges.

THREAT INTELLIGENCE:
A Proof-of-Concept has been developed by the researchers who discovered this vulnerability. There are reports of this vulnerability being actively exploited in the wild in March 2019.

SYSTEM AFFECTED:

- WordPress Easy WP SMTP Plugin 1.3.9 and potentially prior

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in the WordPress Easy WP SMTP Plugin that could allow for remote code execution. This vulnerability exists because the plugin fails to properly authenticate users accessing the admin_init() function in the easy-wp-smtp.php file. An unauthenticated attacker can exploit this issue by crafting an AJAX request to publicly accessible pages that make use of the code including admin-ajax.php and admin-post.php. Successful exploitation of this vulnerability could allow for remote code execution with elevated privileges.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by WordPress manually to affected systems, immediately after appropriate testing.
- Apply the Principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:
WordPress:
https://wordpress.org/plugins/easy-wp-smtp/

Proof of Concept:
https://blog.nintechnet.com/critical-0day-vulnerability-fixed-in-wordpress-easy-wp-smtp-plugin/