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:
04/01/2019

SUBJECT:
Multiple Vulnerabilities in WordPress Social Warfare Plugin Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the WordPress Social Warfare Plugin, the most severe of which could allow for remote code execution. WordPress is a web-based publishing application implemented in PHP, and the Social Warfare Plugin allows users to add social sharing buttons to their content. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution with elevated privileges.

THREAT INTELLIGENCE:
Wordfence has not yet observed RCE activity, but expects new attacks based on the details of the vulnerabilities being published. The developers of the plugin confirmed active exploitation of the plugin's stored cross site scripting vulnerability in the wild in March 2019.

SYSTEM AFFECTED:

- WordPress Social Warfare Plugin versions 3.5.1 and 3.5.2

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:
Multiple vulnerabilities have been discovered in the WordPress Social Warfare Plugin, the most severe of which could allow for remote code execution. This vulnerability exists because the site configuration migration script directly executes attacker-controlled options as PHP code through the use of the PHP eval() function. An unauthenticated attacker can control the options by

submitting a request to the script referencing a malicious configuration file. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution with elevated privileges that could allow the attacker to add administrative users, backdoors, execute system commands, or perform other malicious activity.

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/social-warfare/

Technical Details:
https://www.wordfence.com/blog/2019/03/recent-social-warfare-vulnerability-allowed-remote-code-execution/
https://www.wordfence.com/blog/2019/03/social-warfare-plugin-zero-day-details-and-attack-data/

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/