TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2019-023

DATE(S) ISSUED: 02/20/2019

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

OVERVIEW:
Multiple vulnerabilities have been discovered in WordPress, the most severe of which could allow a WordPress author to execute code remotely on the underlying server. WordPress is a web-based publishing application implemented in PHP. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution with privileges of the affected application.

THREAT INTELLIGENCE:
A Proof-of-Concept has been developed by the researchers who discovered this vulnerability to demonstrate the issues.

SYSTEM AFFECTED:

- WordPress 5 versions prior to 5.0.1
- WordPress 4 versions prior to 4.9.9

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 WordPress that could allow for remote code execution. The vulnerabilities exist because WordPress does not properly validate Post Meta entries submitted by users. This allows an attacker to enter directory traversal sequences for filenames in order to place a malicious file in the WordPress themes directory. Then, an attacker can create a malicious post that includes the malicious file resulting in remote code execution on the underlying host.

- A remote code execution vulnerability due to improper input validation for _wp_attached_file Post Meta entries (CVE-2019-8942)
- A path traversal vulnerability due to improper input validation in the wp_crop_image function (CVE-2019-8943)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution with privileges of the affected application.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate updates provided by WordPress 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 the system before applying patches.

- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:

Proof of Concept:

https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/

CVEs:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8942
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8943

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722