Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

April 07, 2015

Alert Number
I-040715a-PSA

ISIL DEFACEMENTS EXPLOITING WORDPRESS VULNERABILITIES

SUMMARY

Continuous Web site defacements are being perpetrated by individuals sympathetic to the Islamic State in the Levant (ISIL) a.k.a. Islamic State of Iraq and al-Shams (ISIS). The defacements have affected Web site operations and the communication platforms of news organizations, commercial entities, religious institutions, federal/state/local governments, foreign governments, and a variety of other domestic and international Web sites. Although the defacements demonstrate low-level hacking sophistication, they are disruptive and often costly in terms of lost business revenue and expenditures on technical services to repair infected computer systems.

TECHNICAL DETAILS

Researchers continue to identify WordPress Content Management System (CMS) plug-in vulnerabilities, which could allow malicious actors to take control of an affected system. Some of these vulnerabilities were exploited in the recent Web site defacements noted above. Software patches are available for identified vulnerabilities.

Successful exploitation of the vulnerabilities could result in an attacker gaining unauthorized access, bypassing security restrictions, injecting scripts, and stealing cookies from computer systems or network servers. An attacker could install malicious software; manipulate data; or create new accounts with full user privileges for future Web site exploitation.

THREAT

The FBI assesses that the perpetrators are not members of the ISIL terrorist organization. These individuals are hackers using relatively unsophisticated methods to exploit technical vulnerabilities and are utilizing the ISIL name to gain more notoriety than the underlying attack would have otherwise garnered. Methods being utilized by hackers for the defacements indicate that individual Web sites are not being directly targeted by name or business type. All victims of the defacements share common WordPress plug-in vulnerabilities easily exploited by commonly available hacking tools.

DEFENSE

The FBI recommends the following actions be taken:

- Review and follow WordPress guidelines: http://codex.wordpress.org/Hardening_WordPress
- Identify WordPress vulnerabilities using free available tools such as http://www.securityfocus.com/bid, http://cve.mitre.org/index.html, https://www.us-cert.gov/
- Update WordPress by patching vulnerable plugins: https://wordpress.org/plugins/tags/patch
- Run all software as a non-privileged user, without administrative privileges, to diminish the effects of a successful attack

	• Confirm that the operating system and all applications are running the most updated versions