United States Coast Guard

Maritime Cyber Bulletin

Bulletin 003-16 **January 4, 2016**

MARITIME ORGANIZATON'S WEBSITES TARGETED BY ACTORS ATTEMPTING TO EXPLOIT JOOMLA VULNERABILITIES

Overview

This Bulletin is provided to raise awareness of recent malicious cyber activity in the maritime domain and is designed to provide further information about the event and to:

- Provide an overview of current Joomla vulnerabilities being targeted by malicious cyber actors; and
- Provide prevention and mitigation information

Description

Compromised web servers are increasingly being utilized by malicious actors to carry out cyber-attacks, such as distributed denial-of-service attacks against critical infrastructure around the world. These web servers offer increased networking and computing capacity compared with average user workstations, and are therefore a high-value target of choice for malicious actors to build their attack infrastructure. For this reason, it is imperative to secure servers according to best practices, and thus limit their exposure to control by potentially malicious cyber actors.

Specifically, the compromised servers running Content Management Systems (CMSs) are routinely targeted and leveraged as launch points for cyber-attacks. CMSs are software suites that allow site administrators to easily manage the design, functionality, and operation of websites with minimal technical expertise. In recent years, there has been a marked increase in the number of deployments of CMS software on the internet. This has been fueled by popular open source projects which are freely available to users. Unfortunately, some CMS web server operators are not following security best practices, exposing them and others to cyber security risks such as compromise and denial of service.

Joomla is one of the most widely used CMSs in the world. It is PHP-based and allows for the rapid deployment of dynamic content on websites. Joomla has been the subject of a number of vulnerabilities in recent years and, if left unpatched, can represent a risk for site owners and other internet users. Successful exploitation of Joomla vulnerabilities could allow for an attacker to execute arbitrary code in the context of the browser, perform SQL injection, obtain sensitive information, bypass security restrictions, or cause denial of service conditions.

Maritime Event Overview

In late November and early December 2015, the U.S. Coast Guard was notified by a maritime port partner of multiple attempts by cyber actors trying to exploit Joomla vulnerabilities against their company's website(s). During these periods, the company observed 432 attempts to compromise their website(s) via a multitude of attack vectors including SQL injection.

All exploit attempts were unsuccessful.

Technical Details

Current analysis indicates that several versions of Joomla are vulnerable to malicious cyber activities including;

- Joomla versions 1.5 – 3.4.6: Vulnerable to Remote Code Execution
- Joomla versions 3.0.0 – 3.4.6: Vulnerable to SQL Injection

For additional details regarding these vulnerabilities and mitigation users are encouraged to visit the Common Vulnerabilities and Exposures (CVE) website and access vulnerability report CVE-2015-8566.

Risk Mitigation

In general, web site administrators should strive to follow patching instructions from their software providers. Specifically, administrators of Joomla CMS servers should ensure their instillation includes the latest software version available. Additionally, administrators should consider guidance found under the Joomla security section and review the following best practices:

- To the extent possible, maintain moderator control for the creation of user accounts. This may limit the use of automated account creation tools and associated automated posting of malicious content or even site compromise
- Ensure underlying server operating systems, services and software packages, especially third party plugins, are patched and up-to-date
- Apply appropriate Joomla patches after appropriate system/functionality testing
- Verify no unauthorized system modifications have occurred on impacted systems prior to patching
- Ensure accounts and file permissions are set properly, including changing the default administrator user name and password
- Limit version number exposure of extension files by changing their default name to avoid remote automated scanning looking for specific version for which exploits may exist
- Remove unused services and associated files
- Consider deployment of a server security monitoring solution including anti-virus. Additionally, security monitoring and logging including administrative login attempts should be considered
- Monitor intrusion detection systems for signs of anomalous activity
- Review US-CERT's Technical Information Paper TIP-12-298-01 for web site security best practices

Reporting

The U.S. Coast Guard encourages maritime partners to report this type of activity to the National Response Center (NRC) at 1-800-424-8802.

Questions

For maritime cyber safety and security questions or questions related to this report, contact the U.S. Coast Guard Liaison Officer to the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) at:

Email: CGNCCICLNO@hq.dhs.gov

Phone: (703) 235-8850

Feedback

Your feedback is important to us. Please e-mail any comments and/or feedback on this product to CGNCCICLNO@hq.dhs.gov.