Serianu Cyber Security Advisory

Newsletter Plugin Vulnerabilities Affect Over 300,000 Sites

Serianu SOC Advisory Number:

TA – 2020/008

Date Issued:

10th August, 2020

Systems Affected:

- **Newsletter Plugin**

OVERVIEW:

Serianu's Threat Intelligence team uncovered 2 new vulnerabilities in Newsletter plugin, a WordPress plugin with over 300,000 installations. A Newsletter plugin allows you to create subscription forms and send newsletters to your subscribers.

During our investigation of these vulnerabilities, we discovered an unpatched reflected Cross-Site Scripting(XSS) vulnerability and a PHP Object Injection vulnerability. These vulnerabilities could enable the threat actors to implant different backdoors, upload files and take over the admins as it helps to take full control over the website.

This advisory provides an in-depth research on the 2 vulnerabilities in the Newsletter plugin, how they can be exploited and mitigations.

Vulnerabilities Detected

According to our research, there is a firewall rule that protects against the XSS (Cross-site Scripting Vulnerability). This firewall rule was generally obtained by the premium members of the Wordfrence customers on July 15, 2020, and after 30 days, this firewall will be available to all customers without any cost. The PHP Object Injection firewall rule will become available to free Wordfence users on the same date as the XSS rule for this plugin, on August 14, 2020.

1. Authenticated Reflected Cross-Site Scripting(XSS)

Description: Authenticated Reflected Cross-Site Scripting(XSS)
Affected Plugin: Newsletter
Plugin Slug: newsletter
Affected Versions: < 6.8.2
CVE ID: Pending
CVSS Score: 6.5(Medium)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
Fully Patched Version: 6.8.2

A Reflected XSS vulnerability usually relies on an attacker tricking their victim into clicking a malicious link which sends the victim to the vulnerable site along with a malicious payload. This can be done in a number of ways but it is common to first link to an intermediate site controlled by the attacker, which then sends a request containing a malicious payload to the vulnerable site on behalf of the victim.

This could be used in a variety of attacks. For instance, if the victim was a logged-in as an administrator on the vulnerable site, the reflected JavaScript could be used to create a new malicious administrator account controlled by the attacker.

In order for reflected XSS attacks to successfully exploit a user, an attacker needs to trick the user into performing an action. For that reason, Serianu highly recommends users to remain vigilant when clicking on links or attachments in comments, emails, and other communication sources unless you are sure of their integrity and legitimacy.

2. PHP Object Injection

Description: PHP Object Injection
Affected Plugin: Newsletter
Plugin Slug: newsletter
Affected Versions: < 6.8.2
CVE ID: Pending
CVSS Score: 7.5(High)
CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Fully Patched Version: 6.8.2

PHP Object Injection is an application level vulnerability that could allow an attacker to perform different kinds of malicious attacks such as Code Injection, SQL Injection, Path Traversal and Application Denial of Service, depending on the context. The vulnerability occurs when user-supplied input is not properly sanitized before being passed to the unserialize () PHP function. Since PHP allows object serialization, attackers could pass ad-hoc serialized strings to a vulnerable unserialize () call, resulting in an arbitrary PHP object(s) injection into the application scope.

In order to successfully exploit a PHP Object Injection vulnerability two conditions must be met:

- The application must have a class which implements a PHP magic method (such as __wakeup or __destruct) that can be used to carry out malicious attacks, or to start a “POP chain”.
- All of the classes used during the attack must be declared when the vulnerable unserialize () is being called, otherwise object autoloading must be supported for such classes.

Known Vulnerable Software

Software	Version
WordPress	3.6.1
Magento	1.9.0.1
Joomla	3.0.3
IP Board	3.3.4
Dotclear	2.6.1
OpenCart	1.5.6.4
CubeCart	5.2.0
Drupal	7.34
vBulletin	5.1.0
Tuelap	7.6-4
Moodle	2.5.0
WHMCS	5.2.12

Recommendations

Serianu strongly recommends updating to the latest version 6.8.3. of the Newsletter plugin. Users to remain vigilant when clicking on links or attachments in comments, emails, and other communication sources unless you are sure of their integrity and legitimacy.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to Newsletter plugin related vulnerabilities share it with us through our email: info@serianu.com.