Reflected XSS Bug Patched in Popular WooCommerce WordPress Plugin

Author:
Michael Mimoso

August 31, 2017 / 9:30 am

Share this article:

An extension of the WooCommerce WordPress plugin, used by 28 percent of all online stores, has been patched against a reflected cross-site scripting vulnerability.

The vulnerability was found in the Product Vendors plugin, which allows an existing ecommerce site to support multiple vendors, products and payment options. Versions 2.0.35 and earlier are affected by this vulnerability, and site owners are urged to patch immediately.

Automatic updates are available, but are dependent on a site's configuration, and many site operators do not enable them.

"At the time of discovery it was a zero day on the current version," said Logan Kipp, WordPress evangelist for security vendor SiteLock. "If this was discovered by someone else, it could have been a real problem."

Kipp said the reflected XSS bug was found in a particular field on the sign-up form available for new vendors through the plugin.

"Theoretically, this is weaponizable by sending a crafted link to any party who has a set of logins on that website," Kipp said. "And if they have an active session, you could hijack that session."

An attacker could email that crafted link to an already established vendor on a site running WooCommerce. If the vendor is logged in and clicks on the link, an attacker could capture the session and run scripts on the vendor's browser, taking control of any functionality they have, Kipp explained.

"The chances are very high that if they are the webmaster, they're going to be logged in at the time of clicking the link and they're going to have very high privileges," Kipp said. Kipp characterizes XSS as a tool to gain higher privileges.

"It's a means to go further, a foothold," he said. "So while in itself it may not cause any direct damage to the website, we could potentially gain administrator privileges by hijacking sessions."

Unlike persistent cross-site scripting bugs where an attacker can drop arbitrary code on a site through some interaction that was not filtered, reflected XSS means that an attacker can inject executable code only onto a session rather than into the application. These types of attacks are more common, Kipp said.

An attacker can craft a URL, for example in this case, to automatically submit the entries they put into the form so that as soon as a victim clicks on the link, the malicious script is executed. In the case of the WooCommerce plugin, there's a high chance of potential vendors having a question about the form and luring the site admin to execute a malicious script.

The vulnerability was disclosed to Automattic, the parent company behind WooCommerce, through its HackerOne bug bounty program. SiteLock was awarded a $225 which it donated to the WordPress Foundation.

"The great thing about patching cross-site scripting vulnerabilities is that it's very simple inside your own code," Kipp said. "It's all about properly sanitizing the interactive arguments. In this case, it's interesting to find that every other field of this form was properly sanitized with the exception of this one. It's common to see this. It was probably a feature added after they developed the extension, probably by a second developer who did not follow the same practices."

Vulnerabilities Web Security

SUGGESTED ARTICLES

Critical WordPress-Plugin Bug Found in 'Orbit Fox' Allows Site Takeover

Two security vulnerabilities — one a privilege-escalation problem and the other a stored XSS bug — afflict a WordPress plugin with 40,000 installs.

January 13, 2021

6 Questions Attackers Ask Before Choosing an Asset to Exploit

David "moose" Wolpoff at Randori explains how hackers pick their targets, and how understanding "hacker logic" can help prioritize defenses.

December 29, 2020 2

5M WordPress Site 'Contact Form 7' F to Attack

A critical unrestricted fil Contact Form 7 allows a unauthenticated visitor site running the plugin.

December 17, 2020

INFOSEC INSIDER

Securing Your Move to the Hybrid Cloud

August 1, 2022

Why Physical Security Maintenance Should Never Be an Afterthought

July 25, 2022

July 12, 2022

Rethinking Vulnerability Management in a Heightened Threat Landscape

July 11, 2022