

Components:

givewp givewp *

Description:

The Donations Widget plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.19.4 via deserialization of untrusted input from the Donation Form through the 'card\address' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to achieve remote code execution.

Main problems:

502 "Deserialization of Untrusted Data"