

```
givewp givewp *
```

### Description:

The GiveWP Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.19.2 via deserialization of untrusted input from the donation form like 'firstName'. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to delete arbitrary files on the server that makes remote code execution possible. Please note this was only partially patched in 3.19.3, a fully sufficient patch was not released until 3.19.4. However, another CVE was assigned by another CNA for version 3.19.3 so we will leave this as affecting 3.19.2 and before. We have recommended the vendor use JSON encoding to prevent any further deserialization vulnerabilities from being present.

### Main problems:

502 "Deserialization of Untrusted Data"