Advisory: CVE-2020-29045 - Unauthenticated RCE via Arbitrary Object Deserialisation in Five Star Restaurant Menu - WordPress Ordering Plugin

Research / Security Alerts / Posted March 10, 2021

It is possible to gain **Unauthenticated** Remote Code Execution (RCE) on any **WordPress** instance that is using this plugin, due to the unsafe use of *unserialize* for the parsing of unsanitised user input, via the cookie *fdm_cart* used within *includes/class-cart-manager.php*

CVE: **CVE-2020-29045**
Severity: **HIGH**
Vulnerability Type: **CWE-502**: Deserialization of Untrusted Data
Requires Authentication: **No**

Timeline

Discovered: **2020-11-17** – Nick Blundell, AppCheck Ltd
Contacted Vendor (with no response): **2020-11-17** and again on **2020-11-30**
Reported directly to **WordPress Security Team**: **2021-01-06**
Fixed: **2021-01-11** (in version **2.2.1**)

Affected Software

Name: **Five Star Restaurant Menu – WordPress Ordering Plugin**
URL: https://wordpress.org/plugins/food-and-drink-menu/
Version: **<= 2.2.0**
Vendor: **Fivestar Plugins** (https://www.fivestarplugins.com/)
Google dork: inurl:"/wp-content/plugins/food-and-drink-menu/"

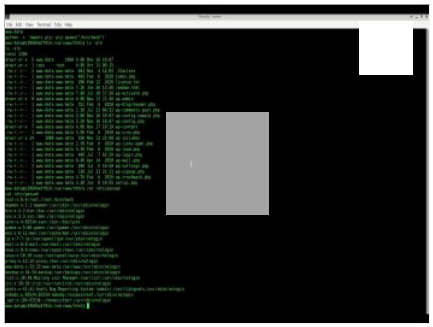
Affected Components

The following code **deserialises** the cookie value sent from the user, such that **arbitrary code** may be injected:

```
1.  // File: includes/class-cart-manager.php
2.
3.  public function load_cart_from_cookie() {
4.
5.          $fdm_cart_items = isset( $_COOKIE['fdm_cart'] ) ? unserialize( $_COOKIE['fdm_cart'] ) : array();
6.          // -->                                              ^^^^^^^^^^^
7.          if ( ! is_array( $fdm_cart_items ) ) { return; }
8.
9.          foreach ( $fdm_cart_items as $fdm_cart_item ) {
10.             $this->cart_items[ $fdm_cart_item->item_identifier ] = $fdm_cart_item;
11.         }
12.     }
```

Exploitation Demo

Exploitation of PHP serialisation vulnerabilities involves leveraging a collection of *gadget* classes that are already present within the vulnerable application, such as third party libraries, in such a way that arbitrary code execution (or some other malicious action) is executed when that *chain* of gadget classes is *deserialised*. See references below for more details on this class of vulnerability and its exploitation.



Exploit Demo Screencast

References

- https://plugins.svn.wordpress.org/food-and-drink-menu/tags/2.2.0/includes/class-cart-manager.php#line-21
- https://plugins.trac.wordpress.org/changeset/2454057/food-and-drink-menu#file3
- https://owasp.org/www-community/vulnerabilities/PHP_Object_Injection
- https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization
- https://notsosecure.com/remote-code-execution-via-php-unserialize/
- https://nitesculucian.github.io/2018/10/05/php-object-injection-cheat-sheet/
- https://www.php.net/manual/en/language.oop5.magic.php
- https://vickieli.medium.com/diving-into-unserialize-pop-chains-35bc1141b69a

About AppCheck

AppCheck is a software security vendor based in the UK, that offers a leading security scanning platform that automates the discovery of security flaws within organisations websites, applications, network, and cloud infrastructure.

As always, if you require any more information on this topic or want to see what unexpected vulnerabilities AppCheck can pick up in your website and applications then please get in contact with us: info@appcheck-ng.com

No software to download or install.
Contact us or call us 0113 887 8380

Start your free trial

POPULAR

DNS Security

The New OpenSSL Critical Vulnerability - Early Information and Detections

File Upload Vulnerabilities

RECENT ARTICLES

DNS Security

The New OpenSSL Critical Vulnerability - Early Information and Detections

File Upload Vulnerabilities

RELATED

File Upload Vulnerabilities

What is Open-Source Intelligence (OSINT)?

World's Strangest Hacks