Ram Gall

November 5, 2020

Object Injection Vulnerability in Welcart e-Commerce Plugin

On October 6, 2020, our Threat Intelligence team discovered a High-Severity Object Injection vulnerability in Welcart e-Commerce, a WordPress plugin with over 20,000 installations that claims top market share in Japan.

After we finished our investigation, we contacted the plugin's publisher, Collne Inc. on October 9, 2020. Full disclosure was sent on October 12, 2020, and the plugin was patched in version 1.9.36 on October 20, 2020.

Wordfence Premium customers received a firewall rule protecting against this vulnerability on October 9, 2020. Sites still using the free version of Wordfence will receive this rule after 30 days on November 8, 2020.

Description: PHP Object Injection
Affected Products: Welcart e-Commerce
Plugin slug: usc-e-shop
Affected Versions: < 1.9.36
CVE ID: CVE-2020-28339
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: 1.9.36

Welcart e-Commerce is a WordPress plugin that can be used to create an online store with a separate customer account area. It uses its own cookies, separate from the ones used by WordPress, in order to track user sessions. Every request to the site results in the `usces_cookie` being parsed by the `get_cookie` function. This function used `usces_unserialize` to decode the contents of this cookie.

```
1371 | function get_cookie($key='usces_cookie') {
1372 |     $values = isset($_COOKIE[$key]) ? usces_unserialize(stripslashes($_COOKIE[$key])) : NULL;
1373 |     return $values;
1374 | }
```

```
1072 | function usces_unserialize( $data ) {
1073 |     if( is_serialized( $data ) ) {
1074 |         return @unserialize( $data );
1075 |     }
1076 |     if( is_array( $data ) ) {
1077 |         return $data;
1078 |     }
1079 |     return @json_decode( $data, true );
1080 | }
```

Unfortunately, this meant that an attacker could send a request with the `usces_cookie` parameter set to a specially crafted string which, once unserialized, would inject a PHP object.

PHP Object injections require a vulnerable magic method to be present in order to fully exploit what's known as a POP chain. We've mentioned POP chains before in a previous article. A POP chain allows an attacker to make use of what are known as magic methods in order to obtain remote code execution, delete arbitrary files, or perform other actions that could allow them to take over a site.

This plugin included a library, tcpdf, that contains a `__destruct` magic method that could have been used to create a POP chain under other circumstances. Fortunately, a complete POP chain was not present because the plugin unserialized the cookie before the `TCPDF` class was loaded and defined, so it was not possible to inject an object with this class.

In more good news, this vulnerability could not be exploited in conjunction with the recently patched issue in the WordPress core's `Requests_Utility_FilteredIterator` class, since the `usces_unserialize` function used the `is_serialized` function to decide whether to unserialize the cookie data and attacks against `Requests_Utility_FilteredIterator` failed this check.

Timeline

October 6, 2020 – Our Threat Intelligence team discovers a PHP Object Injection vulnerability in Welcart e-Commerce.
October 9, 2020 – Our Threat Intelligence team finishes analyzing the vulnerability and contacts the plugin's publisher. A firewall rule is released for Wordfence Premium users.
October 12, 2020 – We send the full disclosure to the plugin's publisher.
October 20, 2020 – A sufficient patch for Welcart e-Commerce is released.
November 8, 2020 – The Wordfence Firewall rule becomes available to sites running the free version of Wordfence.

Conclusion

In today's article, we detailed a PHP Object in the Welcart e-Commerce plugin. Wordfence Premium users have been protected against this vulnerability since October 9, 2020. Sites still running the free version of Wordfence receive the firewall rule on November 8, 2020.

We highly recommend updating to the latest version, 1.9.36 as of this writing, as soon as possible. If someone you know is using Welcart e-Commerce, we recommend sharing this advisory with them so they can take necessary action to protect their site.

Comments

hsalo *
November 8, 2020
4:46 am

MITRE assigned CVE-2020-28339 for this.

Ram Gall *
November 10, 2020
7:27 am

Hi,

Thanks for bringing this to our attention! The article has been updated with the CVE ID