WordPress WooCommerce Advanced Order Export 3.1.3 Cross Site Scripting

Authored by Jack Misiura

Posted May 5, 2020

WordPress WooCommerce Advanced Order Export plugin version 3.1.3 suffers from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2020-11727
SHA-256 | 1ebb98495b8fa8dad24676dddccc093fc59175e279731d6f0c3ed82e9cbe5251 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Title: Reflected XSS


Product: WordPress WooCommerce - Advanced Order Export plugin.


Vendor Homepage: https://algolplus.com/plugins/downloads/advanced-order-export-for-woocommerce-pro/


Vulnerable Version: 3.1.3


Fixed Version: 3.1.4


CVE Number: CVE-2020-11727


Author: Jack Misiura from The Missing Link


Website: https://www.themissinglink.com.au


Timeline:


2020-04-08 Disclosed to Vendor

2020-04-08 Vendor sends fix for testing

2020-04-09 Fix confirmed

2020-04-28 Vendor publishes fix

2020-05-04 Publication


1. Vulnerability Description


The WordPress Advanced Order Export WooCommerce plugin does not sanitise the woe_post_type parameter which can
be passed through in the URL, allowing for HTML or JavaScript injection.


2. PoC


On a WordPress installation with WooCommerce and a vulnerable Advanced Order Export plugin, issue the following
request while logged in as Administrator:

https://wp-site/wp-admin/admin.php?page=wc-order-
export&tab=export&woe_post_type=%22%3E%3Cscript%3Ealert(1);#segment=common


3. Solution


The vendor provides an updated version (3.1.4) which should be installed immediately.


4. Advisory URL


https://www.themissinglink.com.au/security-advisories
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: **December 2022 <**

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	154 files
Ubuntu	73 files
LiquidWorm	23 files
Debian	18 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	8 files
T. Weber	4 files
Julien Ahrens	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed