Payment bypass in WordPress - WooCommerce - NAB Transact plugin disclosure

From: Jack Misiura via Fulldisclosure <fulldisclosure () seclists org>
Date: Thu, 20 Aug 2020 03:16:08 +0000

Title: Payment bypass

Product: WordPress NAB Transact WooCommerce Plugin

Vendor Homepage: https://woocommerce.com/products/nab-transact-direct-post/

Vulnerable Version: 2.1.0

Fixed Version: 2.1.2

CVE Number: CVE-2020-11497

Author: Jack Misiura from The Missing Link

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

Timeline:

2020-03-27 Disclosed to Vendor

2020-03-29 Vendor publishes first fix

2020-04-04 Vendor publishes second fix

2020-08-17 Fix confirmed

2020-08-20 Publication

1. Vulnerability Description

The WordPress NAB Transact WooCommerce plugin does not validate the origin of payment processor status requests, allowing orders to be marked as fully paid by issuing a specially crafted GET request during the ordering workflow.

2. PoC

When presented with a payment screen, instead of submitting payment information, issue the following GET request to
the
site:

```
https://example-site.com/?wc-api=WC_Gateway_Nab_Direct_Post&order=XXXX&key=
wc_order_YYYYY&is_crn=0&txnid=ZZZZZ&refid=WooCommerceXXXX&rescode=00&restext=Approved
```

Where XXXX is the order number and YYYY is the order code which have been present before during the workflow. If these are not presented, submit invalid payment information and get a declined message. Now brute-force the order number which is sequential. Doing so will mark any existing pending orders as fully paid.

3. Solution

The vendor provides an updated version (2.1.2) which should be installed immediately.

4. Advisory URL

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

Jack Misiura

Application Security Consultant

a

9-11 Dickson Avenue

Artarmon

NSW

2064

p

1300 865 865

os

+61 2 8436 8585

w

<https://www.themissinglink.com.au/> themissinglink.com.au

<https://www.linkedin.com/company/the-missing-link-pty-ltd/>

<https://www.facebook.com/The-Missing-Link-268395013346228/?ref=bookmarks>

<https://twitter.com/TML_au>

<https://www.youtube.com/channel/UC2kd4mDmBs3SjW41X3fFHnQ>

<https://www.instagram.com/the_missing_link_it/>

<https://www.themissinglink.com.au/robotic-process-automation>

CAUTION - This message may contain privileged and confidential information intended only for the use of the addressee named above. If you are not the intended recipient of this message you are hereby notified that any use, dissemination,
distribution or reproduction of this message is prohibited. If you have received this message in error please notify The Missing Link immediately. Any views expressed in this message are those of the individual sender and may not necessarily reflect the views of The Missing Link.

themissinglink

Attachment: smime.p7s
Description:

```
_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **Payment bypass in WordPress - WooCommerce - NAB Transact plugin disclosure** *Jack Misiura via Fulldisclosure (Aug 21)*

Install Guide
Docs
Download
Nmap OEM

API docs
Download
Npcap OEM

Full Disclosure
Open Source Security
BreachExchange

Web scanners
Wireless
Exploitation

Advertising
Nmap Public Source License