bug3

Basic Infomation

Download link

```
https://www.dlinktw.com.tw/techsupport/download.ashx?file=3458
```

vulnerability file

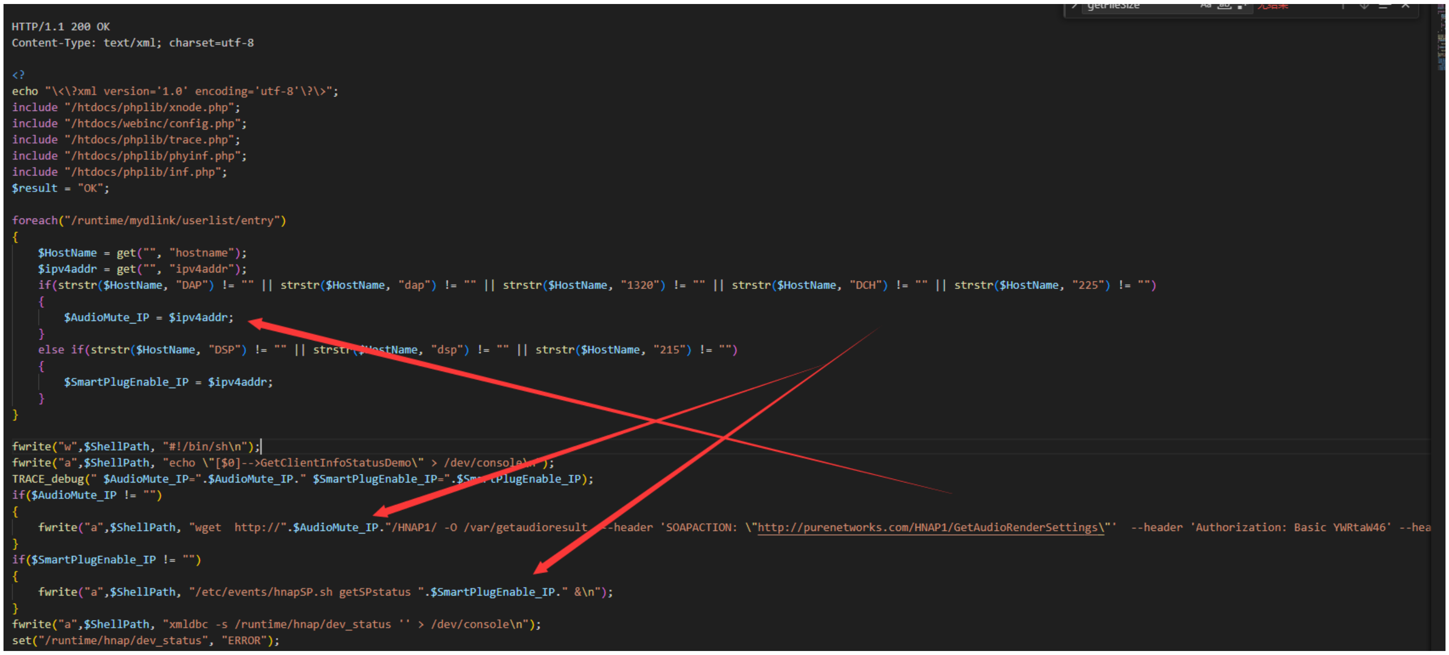
```
GetClientInfoStatusDemo.php
```

vulnerability type

```
command injection
```

Details

ipv4addr can be controlled by the user. The content of ipv4addr in the code is passed to the SmartPlugEnable_IP parameter, and the SmartPlugEnable_IP parameter is used for command execution, so it may lead to malicious code injection.



```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8

<?
echo "\<\?xml version='1.0' encoding='utf-8'\?\>";
include "/htdocs/phplib/xnode.php";
include "/htdocs/webinc/config.php";
include "/htdocs/phplib/trace.php";
include "/htdocs/phplib/phyinf.php";
include "/htdocs/phplib/inf.php";
$result = "OK";

foreach("/runtime/mydlink/userlist/entry")
{
    $HostName = get("", "hostname");
    $ipv4addr = get("", "ipv4addr");
    if(strstr($HostName, "DAP") != "" || strstr($HostName, "dap") != "" || strstr($HostName, "1320") != "" || strstr($HostName, "DCH") != "" || strstr($HostName, "225") != "")
    {
        $AudioMute_IP = $ipv4addr;
    }
    else if(strstr($HostName, "DSP") != "" || strstr($HostName, "dsp") != "" || strstr($HostName, "215") != "")
    {
        $SmartPlugEnable_IP = $ipv4addr;
    }
}

fwrite("w",$ShellPath, "#!/bin/sh\n");
fwrite("a",$ShellPath, "echo \"[$0]-->GetClientInfoStatusDemo\" > /dev/console\n");
TRACE_debug(" $AudioMute_IP=".$AudioMute_IP." $SmartPlugEnable_IP=".$SmartPlugEnable_IP);
if($AudioMute_IP != "")
{
    fwrite("a",$ShellPath, "wget  http://".$AudioMute_IP."/HNAP1/ -O /var/getaudioresult --header 'SOAPACTION: \"http://purenetworks.com/HNAP1/GetAudioRenderSettings\"'  --header 'Authorization: Basic YWRtaW46' --hea
}
if($SmartPlugEnable_IP != "")
{
    fwrite("a",$ShellPath, "/etc/events/hnapSP.sh getSPstatus ".$SmartPlugEnable_IP." &\n");
}
fwrite("a",$ShellPath, "xmldbc -s /runtime/hnap/dev_status '' > /dev/console\n");
set("/runtime/hnap/dev_status", "ERROR");
```

Author