

bug2

Basic Information

Download link

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

vulnerability file

SetVirtualServerSettings.php

function name

getWOLMAC

vulnerability type

command injection

Details

The web parameter LocalIpAddress can be controlled by the user. In the program, ipv4addr obtains this parameter and passes it to the getWOLMAC function for execution. In this case, ipv4addr can inject malicious commands, leading to command injection.

```
function getWOLMAC($ipv4addr)
{
    $cmd = "scut -p ".$ipv4addr." -f 3 /proc/net/arp";
    setattr("/runtime/wakeonlan/mac", "get", $cmd);
    $mac = get("", "/runtime/wakeonlan/mac");
    del("/runtime/wakeonlan/mac");
    return $mac;
}
```

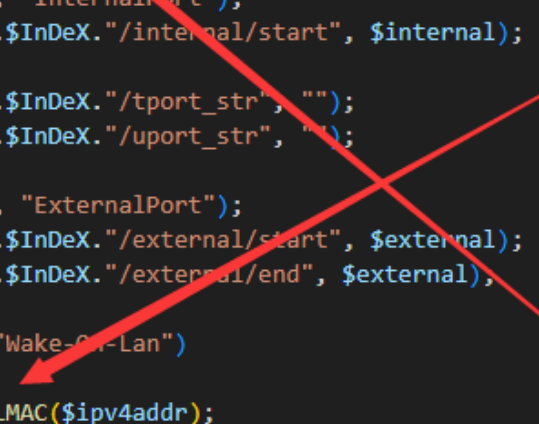
```
set($vsrv_entry." ".$InDeX."/internal/inf", $LAN1);
$ipv4addr = get("x", "LocalIPAddress");
$mask = INF_getcurmask($LAN1);
$hostid = ipv4hostid($ipv4addr, $mask);
set($vsrv_entry." ".$InDeX."/internal/hostid", $hostid);

$internal = get("x", "InternalPort");
set($vsrv_entry." ".$InDeX."/internal/start", $internal);

set($vsrv_entry." ".$InDeX."/tport_str", "");
set($vsrv_entry." ".$InDeX."/uport_str", "");

$external = get("x", "ExternalPort");
set($vsrv_entry." ".$InDeX."/external/start", $external);
set($vsrv_entry." ".$InDeX."/external/end", $external);

if($description == "Wake-On-Lan")
{
    $wolmac = getWOLMAC($ipv4addr);
    set($vsrv_entry." ".$InDeX."/wakeonlan_mac", $wolmac);
}
```



Author

archer@TalentSec Co.,Ltd