



# CVE-2022-48166

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-48166
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-06 22:15:00 UTC
<b>Updated</b>	2023-02-14 20:05:00 UTC
<b>Description</b>	An access control issue in Wavlink WL-WN530HG4 M30HG4.V5030.201217 allows unauthenticated attackers to download

## Risk And Classification

**Problem Types:** CWE-862

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Wavlink</a>	<a href="#">Wl-wn530hg4</a>	-	All	All	All
Operating System	<a href="#">Wavlink</a>	<a href="#">Wl-wn530hg4 Firmware</a>	m30hg4.v5030.201217	All	All	All

## References

Reference	Source	Link	Tags
Broken Access Control - WL-WN530HG4 - Google Docs	MISC	<a href="#">docs.google.com</a>	
Vulns/WAVLINK WN530HG4.md at main · strik3r0x1/Vulns · GitHub	MISC	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)