



CVE-2022-43970

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-43970
State	PUBLIC
Assigner	trelixpsirt@trelix.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-09 21:15:00 UTC
Updated	2023-01-13 14:19:00 UTC
Description	A buffer overflow vulnerability exists in Linksys WRT54GL Wireless-G Broadband Router with firmware <= 4.30.18.006. A s

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Linksys	Wrt54gl	-	All	All	All
Operating System	Linksys	Wrt54gl Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Vuln Research 101 (Part 3) - Hacking the Linksys WRT54GL via buffer overflow - YouTube	CONFIRM	youtu.be	
Vuln Research 101 (Part 2) - Hacking the Linksys WRT54GL via command injection - YouTube	CONFIRM	youtu.be	
Please update your browser	CONFIRM	youtu.be	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

Vendor Comments And Credit

Discovery Credit

LEGACY: Jessie Chick of Trelix ARC

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)