



CVE-2022-46552

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

Summary

CVE	CVE-2022-46552
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-02 13:15:00 UTC
Updated	2023-04-05 18:15:00 UTC
Description	D-Link DIR-846 Firmware FW100A53DBR was discovered to contain a remote command execution (RCE) vulnerability via

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir-846	-	All	All	All
Operating System	Dlink	Dir-846 Firmware	100a53db	All	All	All

References

Reference

D-Link DIR-846 Remote Command Execution ~ Packet Storm

Security Bulletin | D-Link

CVE-2022-46552 | D-Link DIR-846 Wireless Router in firmware FW100A53DBR-Retail has a vulnerability that lead to a RCE | by Franoa Tat

phpcs-security-audit/SystemExecFunctionsSniff.php at master · FloeDesignTechnologies/phpcs-security-audit · GitHub

cve-reported/CVE-2022-46552.md at main · c2dc/cve-reported · GitHub

PHP: Program execution Functions - Manual

CWE - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (4.9)

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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](#)