



CVE-2021-27342

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

Summary

CVE	CVE-2021-27342
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-17 13:15:00 UTC
Updated	2021-05-24 20:14:00 UTC
Description	An authentication brute-force protection mechanism bypass in telnetd in D-Link Router model DIR-842 firmware version 3.0

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir-842e	r1	All	All	All
Operating System	Dlink	Dir-842e Firmware	All	All	All	All

References

Reference	Source
D-Link Router CVE-2021-27342 Vulnerability Writeup	MITRE
D-Link-CVE-2021-27342-exploit/dlink-telnet-exploit-CVE-2021-27342.py at main · guywhataguy/D-Link-CVE-2021-27342-exploit · GitHub	MITRE
D-Link Technical Support	CVE
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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