



CVE-2019-17525

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

Summary

CVE	CVE-2019-17525
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-21 19:15:00 UTC
Updated	2020-06-04 21:15:00 UTC
Description	The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism

Risk And Classification

Problem Types: CWE-307

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir-615	t1	All	All	All
Hardware	Dlink	Dir-615	t1	All	All	All
Operating System	Dlink	Dir-615 Firmware	20.10	All	All	All
Operating System	Dlink	Dir-615 Firmware	20.10	All	All	All

References

Reference

- [GitHub - huzzaifahussain98/CVE-2019-17525: D-LINK ROUTER "MODEL NO: DIR-615" with "FIRMWARE VERSION:20.10" & "HARDWARE VERSION:20.10"](#)
- [D-Link DIR-615 T1 20.10 CAPTCHA Bypass ≈ Packet Storm](#)
- [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](#).

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