



# CVE-2020-29557

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-29557
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-29 20:15:00 UTC
<b>Updated</b>	2023-04-27 14:31:00 UTC
<b>Description</b>	An issue was discovered on D-Link DIR-825 R1 devices through 3.0.1 before 2020-11-20. A buffer overflow in the web inter

## Risk And Classification

**EPSS:** 0.910330000 probability, percentile 0.996420000 (date 2026-04-22)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-119

## CISA Known Exploited Vulnerability

<b>Vendor</b>	D-Link
<b>Product</b>	DIR-825 R1 Devices
<b>Name</b>	D-Link DIR-825 R1 Devices Buffer Overflow Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-29557">https://nvd.nist.gov/vuln/detail/CVE-2020-29557</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825</a>	r1	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825</a>	r1	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/a</a>	d1a	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/a</a>	d1a	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/ac</a>	e	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/ac</a>	e1a	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/ac</a>	e	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/ac</a>	e1a	All	All	All

Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/acf</a>	f1	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/acf</a>	f1	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/gf</a>	gf	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-825/gf</a>	gf	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dir-825 R1 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-825</a>	r1	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-825/a</a>	d1a	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-825/ac</a>	e	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-825/ac</a>	e1a	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-825/acf</a>	f1	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-825/gf</a>	gf	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dir-825 R1 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Reversing DIR-825 Dlink router – Shaked Delarea – Security Researcher	MISC	<a href="https://shaqed.github.io">shaqed.github.io</a>	Exploit, Third Party Advisory
D-Link Загрузки	MISC	<a href="http://www.dlink.ru">www.dlink.ru</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>	kev

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](https://cve.report/api)

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