



CVE-2021-42784

Published on: Not Yet Published

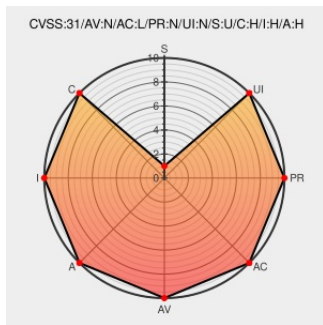
Last Modified on: 11/29/2021 02:18:00 PM UTC

CVE-2021-42784

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Dwr-932c](#) from [Dlink](#) contain the following vulnerability:

OS Command Injection vulnerability in debug_fcgi of D-Link DWR-932C E1 firmware allows a remote attacker to perform command injection via a crafted HTTP request.

CVE-2021-42784 has been assigned by cve_disclosure@tech.gov.sg to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [D-Link](#) - **DWR-932C E1** version **<= 1.0.0.4**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
D-Link Technical Support	supportannouncement.us.dlink.com/text/html	D MISC supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10246

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dwr-932c	revision_e	All	All	All
Operating System	Dlink	Dwr-932c E1 Firmware	All	All	All	All

```
cpe:2.3:h:dlink:dwr-932c:revision_e:*:*:*:*:*:*:
```

```
cpe:2.3:o:dlink:dwr-932c_e1_firmware:*:*:*:*:*:*:
```

Discovery Credit

Eugene Lim from Government Technology Agency of Singapore

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-42784 : OS Command Injection vulnerability in debug_fcgi of D-Link DWR-932C E1 firmware allows a remote at... twitter.com/i/web/status/1...	2021-11-23 22:02:41
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-42784 Description: OS Command Injection vulnerability in debug_fcgi of... twitter.com/i/web/status/1...	2021-11-23 23:00:08
@LinInfoSec	Dwr - CVE-2021-42784: supportannouncement.us.dlink.com/announcement/p...	2021-11-23 23:53:00

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 [TW](#) [NI](#) |

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