



CVE-2022-36785

Published on: Not Yet Published

Last Modified on: 10/25/2023 06:17:00 PM UTC

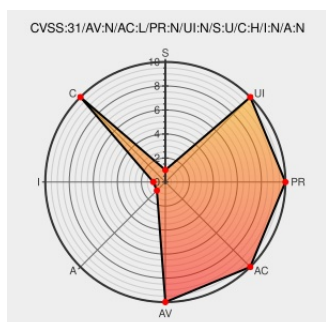
CVE-2022-36785 - advisory for ILVN-2022-0056

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [G Integrated Access Device4](#) from [Dlink](#) contain the following vulnerability:

D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass. *Information Disclosure – file contains a URL with private IP at line 15 "login.asp" A. The window.location.href = http://192.168.1.1/setupWizard.asp"

http://192.168.1.1/setupWizard.asp" ; "admin" – contains default

username value "login.asp" B. While accessing the web interface, the login form at *Authorization Bypass – URL by "setupWizard.asp" while it blocks direct access to – the web interface does not properly validate user identity variables values located at the client side, it is available to access it without a "login_glag" and "login_status" checking browser and to read the admin user credentials for the web interface.

CVE-2022-36785 has been assigned by [cna@cyber.gov.il](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [D-Link](#) - **G integrated Access Device4** version < **Upgrade to the latest version.**

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Attention Required! Cloudflare	web.archive.org text/html Inactive Link Not Archived	MISC www.gov.il/en/Departments/faq/cve_advisories

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	G Integrated Access Device4	-	All	All	All
Operating System	Dlink	G Integrated Access Device4 Firmware	1.0	All	All	All
cpe:2.3:h:dlink:g_integrated_access_device4:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:dlink:g_integrated_access_device4_firmware:1.0:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-36785 : D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass. *Information D... twitter.com/i/web/status/1...	2022-11-17 23:07:29

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)