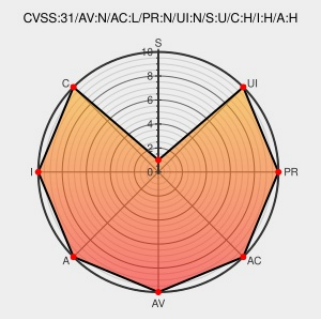
CVE-2023-32222

Published on: Not Yet Published

Last Modified on: 07/06/2023 03:34:00 PM UTC

CVE-2023-32222

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dsl-g256dg from Dlink contain the following vulnerability:

D-Link DSL-G256DG version vBZ_1.00.27 web management interface allows authentication bypass via an unspecified method.

CVE-2023-32222 has been assigned by cna@cyber.gov.il to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **D-Link** - **DSL-G256DG firmware version vBZ_1.00.27** version **>= Manufacturer recommends replacing the unit.**

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

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	Dsl-g256dg	-	All	All	All
Operating System	Dlink	Dsl-g256dg Firmware	bz_1.00.27	All	All	All

cpe:2.3:h:dlink:dsl-g256dg:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dsl-g256dg_firmware:bz_1.00.27:*:*:*:*:*:*:*:

Discovery Credit

Daniel Levi

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-32222 : D-Link DSL-G256DG version vBZ_1.00.27 web management interface allows authentication bypass via an… twitter.com/i/web/status/1…	2023-06-28 21:06:38
@cracbot	CVE-2023-32222 (CVSS:9.8, CRITICAL) is Received. D-Link DSL-G256DG version vBZ_1.00.27 web management interface all… twitter.com/i/web/status/1…	2023-06-29 06:00:14
@leak_ix	⚠ Update your D-LINK routers, CVE-2023-32222 -> Web management interface allows authentication bypass via an unspe… twitter.com/i/web/status/1…	2023-06-29 10:31:48
@samilaiho	D-Link DSL-G256DG firmware version vBZ_1.00.27 URL: Classification: Critical, Solution: Una… twitter.com/i/web/status/1…	2023-06-30 05:22:15
@vuldb	There is a new vulnerability with elevated criticality in D-Link DSL-G256DG (CVE-2023-32222) vuldb.com/?id.232661	2023-06-30 05:58:02

← Previous ID

Next ID→