

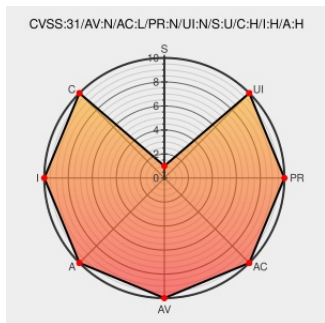


CVE-2018-20432

Published on: 09/14/2020 12:00:00 AM UTC

Last Modified on: 11/16/2022 02:48:00 PM UTC

CVE-2018-20432

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Covr-2600r](#) from [Dlink](#) contain the following vulnerability:

D-Link COVR-2600R and COVR-3902 Kit before 1.01b05Beta01 use hardcoded credentials for telnet connection, which allows unauthenticated attackers to gain privileged access to the router, and to extract sensitive data or modify the configuration.

CVE-2018-20432 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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
CVE-2018-20432 - Hardcoded credentials in DLink CoVR-2600R Router	cybersecurityworks.com text/html	csw MISC cybersecurityworks.com/zeroday/cve-2018-20432-dlink.html
COVR 3902 1.01B0 Hardcoded	Exploit	PS MISC packetstormsecurity.com/files/159058/COVR-3902-1.01B0-

Credentials ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	Hardcoded-Credentials.html
D-Link Technical Support	Patch Vendor Advisory supportannouncement.us.dlink.com text/html	MISC supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10109

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	Covr-2600r	-	All	All	All
Hardware 	Dlink	Covr-2600r	-	All	All	All
Operating System	Dlink	Covr-2600r Firmware	All	All	All	All
Hardware 	Dlink	Covr-3902	-	All	All	All
Hardware 	Dlink	Covr-3902	-	All	All	All
Operating System	Dlink	Covr-3902 Firmware	All	All	All	All
cpe:2.3:h:dlink:covr-2600r:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:dlink:covr-2600r:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:dlink:covr-2600r_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:dlink:covr-3902:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:dlink:covr-3902:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:dlink:covr-3902_firmware:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)