

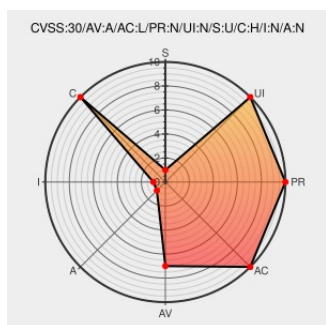


CVE-2020-27863

Published on: 02/11/2021 12:00:00 AM UTC

Last Modified on: 04/23/2021 05:28:00 PM UTC

CVE-2020-27863

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

Certain versions of [Dsl-2888a](#) from [Dlink](#) contain the following vulnerability:

This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DVA-2800 and DSL-2888A routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the dhttpd service, which listens on TCP port 8008 by default. The issue results from incorrect

string matching logic when accessing protected pages. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10912.

CVE-2020-27863 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **D-Link - Multiple Routers** version **firmware version 2.3**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
D-Link Technical Support	Vendor Advisory supportannouncement.us.dlink.com text/html	 MISC supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10196
ZDI-20-1427 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-20-1427/

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-2888a	revision_t	All	All	All
Hardware 	Dlink	Dsl-2888a	revision_t	All	All	All
Operating System	Dlink	Dsl-2888a Firmware	2.30_au	All	All	All
Operating System	Dlink	Dsl-2888a Firmware	2.30_au	All	All	All
Hardware 	Dlink	Dva-2800	revision_t	All	All	All
Hardware 	Dlink	Dva-2800	revision_t	All	All	All
Operating System	Dlink	Dva-2800 Firmware	2.30_au	All	All	All
Operating System	Dlink	Dva-2800 Firmware	2.30_au	All	All	All

```
cpe:2.3:h:dlink:dsl-2888a:revision_1:***.***.***.***
```

```
cpe:2.3:h:dlink:dsl-2888a:revision_1.*.*.*.*.*:
```

```
cpe:2.3:o:dlink:dsl-2888a_firmware:2.30_au:*.*.*.*.*:
```

```
cpe:2.3:o:dlink:dsl-2888a_firmware:2.30_au:*:*:*:*:
```

```
cpe:2.3:h:dlink:dva-2800:revision_t:*****:
```

cpe:2.3:h:dlink:dva-2800:revision_t:.*:.*:.*:.*:.*:.*

```
cpe:2.3:o:dlink:dva-2800_firmware:2.30_au:*:*:*:*:*:
```

```
cpe:2.3:o:dlink:dva-2800_firmware:2.30_au:****:*:
```

chung96vn ft phieulang

[← 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](#)