



# CVE-2020-24580

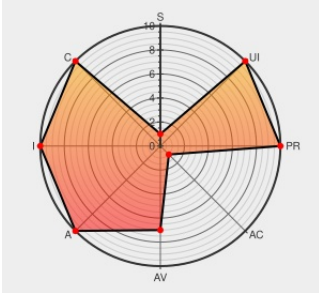
Published on: 12/22/2020 12:00:00 AM UTC

Last Modified on: 04/26/2023 07:27:00 PM UTC

## CVE-2020-24580

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

CVSS:31/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Dsl2888a](#) from [D-link](#) contain the following vulnerability:

An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU\_2.31\_V1.1.47ae55. Lack of authentication functionality allows an attacker to assign a static IP address that was once used by a valid user.

CVE-2020-24580 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector           | Attack Complexity      | Privileges Required | User Interaction    |
|-------------------------|------------------------|---------------------|---------------------|
| <b>ADJACENT_NETWORK</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |
| Scope                   | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b>        | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **5.4 - MEDIUM**

| Access Vector           | Access Complexity | Authentication      |
|-------------------------|-------------------|---------------------|
| <b>ADJACENT_NETWORK</b> | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact  | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>          | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                               | Tags                                                                                                   | Link                                                                                              |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Security Advisories   Trustwave           | <a href="#">Third Party Advisory</a><br><a href="#">www.trustwave.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM www.trustwave.com/en-us/resources/security-resources/security-advisories/</a> |
| D-Link: Multiple Security Vulnerabilities | <a href="#">Exploit</a>                                                                                | <a href="#">MISC www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/d-</a>                   |

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](mailto: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   | D-link | Dsl2888a          | -       | All    | All     | All      |
| Hardware   | D-link | Dsl2888a          | -       | All    | All     | All      |
| Operating System                                                                            | D-link | Dsl2888a Firmware | All     | All    | All     | All      |
| Operating System                                                                            | D-link | Dsl2888a Firmware | All     | All    | All     | All      |
| Hardware  | Dlink  | Dsl2888a          | -       | All    | All     | All      |
| Operating System                                                                            | Dlink  | Dsl2888a Firmware | All     | All    | All     | All      |
| cpe:2.3:h:d-link:dsl2888a:-:~::~~::~~::~~::~~::~~::~~:::                                    |        |                   |         |        |         |          |
| cpe:2.3:h:d-link:dsl2888a:-:~::~~::~~::~~::~~::~~::~~:::                                    |        |                   |         |        |         |          |
| cpe:2.3:o:d-link:dsl2888a_firmware:~::~~::~~::~~::~~::~~::~~:::                             |        |                   |         |        |         |          |
| cpe:2.3:o:d-link:dsl2888a_firmware:~::~~::~~::~~::~~::~~::~~:::                             |        |                   |         |        |         |          |
| cpe:2.3:h:dlink:dsl2888a:-:~::~~::~~::~~::~~::~~::~~:::                                     |        |                   |         |        |         |          |
| cpe:2.3:o:dlink:dsl2888a_firmware:~::~~::~~::~~::~~::~~::~~:::                              |        |                   |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→