



# CVE-2025-50654

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

| Summary         |                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2025-50654                                                                                                                 |
| State           | PUBLISHED                                                                                                                      |
| Assigner        | mitre                                                                                                                          |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                   |
| Published       | 2026-04-08 19:24:16 UTC                                                                                                        |
| Updated         | 2026-04-22 16:16:50 UTC                                                                                                        |
| Description     | A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper validation of the id parameter in the /thd |

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.000500000 probability, percentile 0.155020000 (date 2026-04-22)

Problem Types: CWE-120 | n/a | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov                         | Primary   | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1     | ADP                                  | DECLARED  | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

| CVSS v3.1 Breakdown |           |
|---------------------|-----------|
| Attack Vector       | Network   |
| Attack Complexity   | Low       |
| Privileges Required | None      |
| User Interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     |           |

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

#### NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                | Product                          | Version    | Update | Edition | Language |
|------------------|-----------------------|----------------------------------|------------|--------|---------|----------|
| Hardware         | <a href="#">Dlink</a> | <a href="#">Di-8003</a>          | -          | All    | All     | All      |
| Operating System | <a href="#">Dlink</a> | <a href="#">Di-8003 Firmware</a> | 16.07.26a1 | All    | All     | All      |

#### Vendor Declared Affected Products

| Source | Vendor             | Product             | Version      | Platforms     |
|--------|--------------------|---------------------|--------------|---------------|
| CNA    | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

#### References

| Reference                                                                           | Source                        | Link                                             | Tags           |
|-------------------------------------------------------------------------------------|-------------------------------|--------------------------------------------------|----------------|
| <a href="#">github.com/xiaotea/iot-vulnerability-collection/blob/main/README.md</a> | <a href="#">cve@mitre.org</a> | <a href="#">github.com</a>                       | Third Party Ac |
| <a href="#">supportannouncement.us.dlink.com/security/publication.aspx</a>          | <a href="#">cve@mitre.org</a> | <a href="#">supportannouncement.us.dlink.com</a> |                |
| <a href="#">www.dlink.com/en/security-bulletin</a>                                  | <a href="#">cve@mitre.org</a> | <a href="#">www.dlink.com</a>                    | Vendor Advise  |
| CVE Program record                                                                  | <a href="#">CVE.ORG</a>       | <a href="#">www.cve.org</a>                      | canonical      |
| NVD vulnerability detail                                                            | <a href="#">NVD</a>           | <a href="#">nvd.nist.gov</a>                     | canonical, and |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)