



zuhri / **advisory**

📡
👁️
1
☆
0
🔗
0

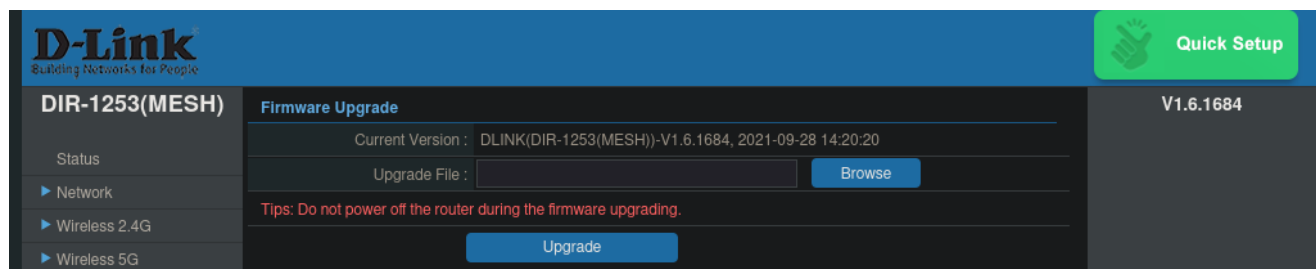
<> **Code** ↶ Activity

🔗 main
advisory / CVE-2025-29165
📄
🕒 History
⋮

| | |
|--------------------------------|---------------|
| zuhri update references | two weeks ago |
| ← .. | |
| .assets | last month |
| CVE-2025-29165 | last month |
| DLINK_N2M_ID_V1.6.1684... | last month |
| README.md | two weeks ago |

📖 README.md

CVE-2025-29165



Hardcoded Credential on DLINK DIR-1253 Firmware

Prior version \leq V1.6.1684 DLINK DIR-1253 vulnerable to information disclosure (Hardcoded Credential). The file affected at `/etc/shadow.sample` contained a hardcoded `root` credential. These credentials are used in `/var/shadow` by the following `/init.d/rcS_{AP,GW}` boot script, this script is being execute when booting process is start.

Proof of Concept

A fully automate PoC script.

```
zuhri@advisory:~/PoC/CVE-2025-29165$ []  
  
[0] 0:sh* 1:sh- "" 13:26 06-Mar-26
```

find more vulnerability detail at <https://zuh.re/cve/2025-29165>.

Conclusion

This vulnerability allows an attacker to compromise root access level via tty (TTL pin) as example, which will turn into arbitrary attack vector.

References

- [NIST: CVE-2024-37630](#)
- [MITRE: CWE-276](#)
- [MITRE: CWE-798](#)

Link Firmware

- <https://github.com/rhpz/DIR-1253>
- <https://archive.org/details/dir-1253-m-dlink-id-v-1.6.1527>

Codeberg

[Blog](#)

[Documentation](#)

[Community Issues](#)

[Contributing](#)

[Report Abuse](#)

Association

[Who are we?](#)

[Bylaws / Satzung](#)

[Donate](#)

[Join / Support](#)

[Contact](#)

Services

[Codeberg Pages](#)

[Codeberg Translate](#)

[Woodpecker CI](#)

[Forgejo API](#)

[Status Page](#)

Legal

[Imprint / Impressum](#)


[Privacy Policy](#)

[Licenses](#)

[Terms of Use](#)

[Mastodon](#) | [Matrix Space \(Web link\)](#) 

Powered by [Forgejo](#)

 English

