COMMUNITY CONTENT

Home › Submit › 790290

Submit #790290: D-Link DIR-882 1.01B02 OS Command Injection

Title	D-Link DIR-882 1.01B02 OS Command Injection
Description	A command injection vulnerability was identified in D-Link DIR-882 Rev. A1 firmware v1.01B02. The HNAP1 SetNetworkSettings handler passes the user-supplied IPAddress parameter unsanitized into sprintf() and then system() in prog.cgi at offset 0x43511C. The only validation performed is a minimum string length check (>=7 characters). An authenticated attacker can inject arbitrary OS commands via shell metacharacters in the IPAddress field, achieving remote code execution as root. Exploitation was verified in QEMU emulation with GDB breakpoints confirming the injected payload reaching system().
Source	https://files.catbox.moe/ei31k1.zip
User	meshaal (UID 96796)
Submission	03/26/2026 05:39 PM (14 days ago)
Moderation	04/08/2026 08:44 PM (13 days later)
Status	Accepted
VulDB entry	[D-Link DIR-882 1.01B02 HNAP1 SetNetworkSettings prog.cgi sprintf IPAddress os command injection]
Points	17

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling