COMMUNITY CONTENT

Home › Submit › 788298

Submit #788298: D-Link DIR-645 1.01–1.03 Stack-based Buffer Overflow

Title	D-Link DIR-645 1.01–1.03 Stack-based Buffer Overflow
Description	The D-Link DIR-600 is a wireless router designed for home and small office environments, and it is still deployed in some actual network scenarios. In early firmware versions of the D-Link DIR-645 router (such as v1.01–v1.03), the core function `hedwigcgi_main` of `/cgi-bin/hedwig.cgi` has a stack-based buffer overflow vulnerability. When processing HTTP requests, the program retrieves the user session identifier (Session UID), which can be indirectly controlled by client requests. Then, it uses `sprintf` to concatenate it into a fixed-size stack buffer without performing length checks. If an attacker constructs overly long input, it can cause a stack buffer overflow, overwriting registers and the return address ($ra) on the stack, thereby hijacking the program's execution flow. By carefully crafting the data, an attacker can achieve remote code execution (RCE) and ultimately gain full control of the device.
Source	https://github.com/Pers1st0/CVE/blob/main/stack-based%20buffer%20overflow%20vulnerability%20exists%20in%20the%20hedwig.cgi%20of%20D-Link%20DIR-645.md
User	Pers1st (UID 98793)
Submission	03/25/2026 01:01 PM (14 days ago)
Moderation	04/08/2026 05:30 PM (14 days later)
Status	Accepted
VulDB entry	[D-Link DIR-645 1.01/1.02/1.03 /cgi-bin/hedwig.cgi hedwigcgi_main stack-based overflow]
Points	20

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