

# Warning: If you own an old D-Link VPN router, throw it away!

The manufacturer has confirmed that a serious vulnerability has been found in some devices that are no longer officially supported.

If you're using an older version of a D-Link VPN router, you might want to think twice before staying connected to the Internet. The manufacturer has confirmed that a serious vulnerability has been found in some devices that are no longer officially supported, so if you own one, you'll want to replace it immediately.

## D-Link Sends Warning to Owners of Its VPN Routers



D-Link has discovered a serious vulnerability in its routers that allows hackers to remotely execute code, one of the most serious cybersecurity vulnerabilities a device can face, The Register reported.

Normally, D-Link would release a patch for affected devices and everything would be fine. However, all of the routers that are affected by this issue are out of date, which means that D-Link cannot release a fix. Therefore, your best bet is to stop using the router altogether and replace it with a supported one.

Here is a list of all the routers that D-Link has sent warnings for, along with the date they were discontinued:

1. DSR-150 (EOL May 2024)

2. DSR-150N (EOL May 2024)
3. DSR-250 (EOL May 2024)
4. DSR-250N (EOL May 2024)
5. DSR-500N (EOL September 2015)
6. DSR-1000N (EOL October 2015)

The vulnerability is so severe that D-Link has refused to provide details about its impact or which parts of the router are affected, out of concern that malicious actors will use the information to attack people's devices.

Fortunately, D-Link is offering affected US users a 20% discount on new, unaffected DSR-250v2 routers, which should make the upgrade much more palatable. You can read about how to claim the discount in D-Link's security notice regarding the bug. Otherwise, if you feel like it's a good time to shop, check out the best Wi-Fi routers of 2024.

You finished reading the article "**Warning: If you own an old D-Link VPN router, throw it away!**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.