Detecting security holes that cause a series of D-Link VPN routers to be remotely attacked

Three new security holes in D-Link's VPN router have just been discovered by security firm Digital Defense.

As revealed by Digital Defense, some of the popular D-Link VPN routers contain serious security vulnerabilities. As a result, millions of home and business networks are at risk of network attack even with strong passwords used.

Immediately after the discovery of security vulnerabilities, on August 11 Digital Defense notified D-Link. If exploited, attackers can remotely access devices on the network and execute arbitrary commands. Hackers can even launch DDoS attacks using the devices themselves.

The routers at risk of being hacked include D-Link DSR-150, DSR-250, DSR-500 and DSR-1000AC and other VPN routers in the DSR family running firmware 3.14 and 3.17.

D-Link confirmed the issue on December 1 and says a fix for 2 of the 3 vulnerabilities has been released. According to D-Link, the third vulnerability won't be patched because it's a feature they're about to implement and its severity has dropped to normal after the latest patch.

Due to the COVID-19 epidemic, the need to work remotely is increasing. Therefore, individuals and businesses also need to use VPN networks. Taking advantage of this, hackers are also actively exploiting the vulnerabilities of the VPN for profit.

To ensure safety, businesses and individuals using these routers should update to the latest firmware from D-Link. Besides, you should regularly check and update the latest software for devices in your network.

tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.