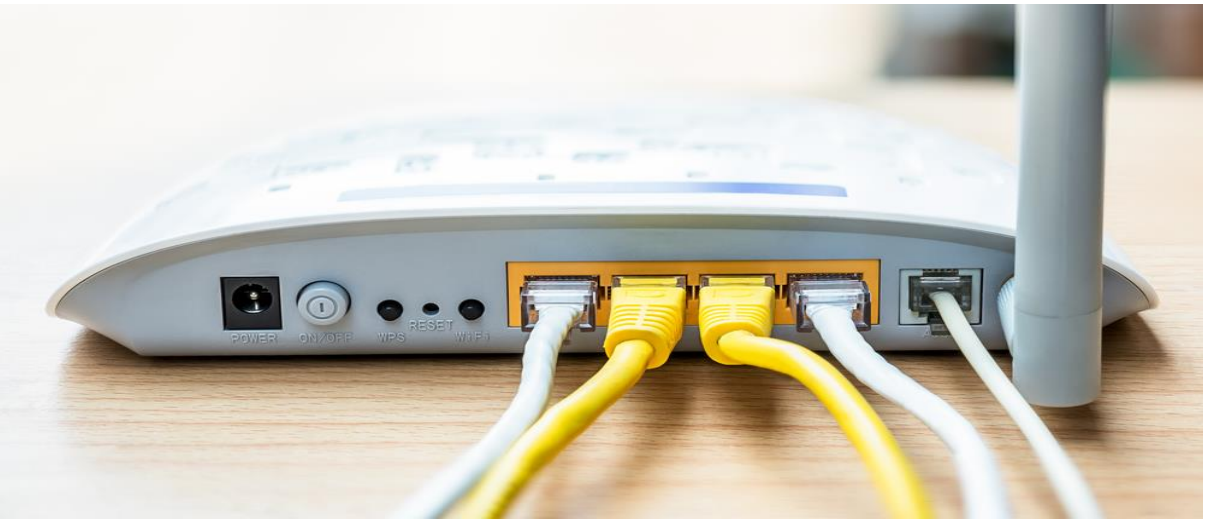
D-Link Partially Patched Severe Security Bugs in Home Routers



During the coronavirus pandemic scenario, any likelihood of attacks against home networks could prove to be a threat against the organizational data as well. So it becomes essential for the vendors to give the same importance to home devices, as is given to enterprise products. But apparently D-Link missed a few loopholes in its patches to DIR-865L home router model, leading to some controversies.

What happened

Some profound bugs were found in the D-Link home routers in Feb 2020. Some of these bugs were patched by the vendor, while some were discarded due to End-of-Support expiry of the product. But now it appears that these bugs may be impacting the latest version of D-Link home routers as well.

In February 2020, Palo Alto Network's Unit 42 researchers had found six new vulnerabilities (CVE-2020-13782, CVE-2020-13783, CVE-2020-13784, CVE-2020-13785, CVE-2020-13786, and CVE-2020-13787) in D-Link wireless cloud routers' D-Link DIR-865L Ax 1.20B01 Beta devices.

In May 2020, D-Link released a beta firmware patch to partially fix only three of the flaws (CVE-2020-13783, CVE-2020-13785, and CVE-2020-13786). D-Link also mentioned that the DIR-865L model has already reached its End-of-Support date in January 2016, and firmware development has ceased for them.

In June 2020, it has been found that these vulnerabilities share a common code base that may also affect newer models as well. Malicious actors can still sniff network traffic to steal session cookies, run arbitrary commands, conduct CSRF, and steal sensitive information by exploiting such vulnerabilities even in the latest models.

Other recent vulnerabilities

Several critical vulnerabilities have been found in D-Link routers earlier as well that allow remote hackers to take control of hardware and steal data.

In January 2020, several D-Link router models were found vulnerable to LiquorBot botnet, that targeted a small set of critical vulnerabilities (CVE-2018-17173, CVE-2017-6884, CVE-2018-10562, CVE-2017-6077, CVE-2017-6334, CVE-2016-5679, CVE-2018-9285, CVE-2013-3568, and CVE-2019-12780).

In the same month, remote command execution (CVE-2019-17621) and information disclosure (CVE-2019-20213) vulnerabilities were found affecting many D-Link routers, mainly the DIR-859 router model.

Security improvements

Users should change the administrative credentials from the default setting, and change the network name, or SSID to something unique. Turning on automatic firmware updates and enabling WPA2 wireless encryption will increase security. Install new firmware as soon as it becomes available.

References:

https://cyware.com/news/d-link-partially-patched-severe-security-bugs-in-home-routers-9b711996

https://www.bleepingcomputer.com/news/security/d-link-leaves-severe-security-bugs-in-home-router-unpatched/

https://www.zdnet.com/article/d-link-routers-contain-remote-code-execution-vulnerability/

https://threatpost.com/work-from-home-alert-critical-d-link-bug/156573/

https://routersecurity.org/bugs.php