Detect dangerous security holes affecting many D-Link routers

Security researchers Miguel Méndez Zúñiga and Pablo Pollanco of Telefónica Chile have just published Proof-of-Concept (PoC) that allows hackers to execute remote commands and exploit vulnerabilities that leak information related to Many D-Link routers are being used worldwide.

Security researchers Miguel Méndez Zúñiga and Pablo Pollanco of Telefónica Chile have just published Proof-of-Concept (PoC) that allows hackers to execute remote commands and exploit vulnerabilities that leak information related to Many D-Link routers are being used worldwide.

The findings of two Chilean security experts were published on the Medium forum, including technical details of the related vulnerabilities along with two videos describing the entire PoC process to exploit the vulnerabilities. this security.

In the above two holes, most notably the remote command execution flaw, tracked with the identifier CVE-2019-17621, resides in the code system used to manage UPnP requests. This vulnerability could be exploited by an unauthentic attacker for the purpose of controlling D-Link router devices, thereby stealing data. However, CVE-2019-17621 can only be exploited by attackers who have access to the same local network segment of the target router.

In other words, to exploit this security flaw, an attacker would have to gain access to the LAN or direct access to the target device, resulting in a significantly reduced attack risk. However, this is still a dangerous flaw.

D-Link was notified by a third-party company about CVE-2019-17621 in mid-October, but the initial security advisor determined that the DIR-859 router series was vulnerable. Actual tests later revealed that dozens of D-Link DIR models were on the list of vulnerable devices.

The remaining flaw - CVE-2019-20213 - could reveal sensitive information to an attacker if it is successfully exploited, including the device's VPN configuration file, and many other sensitive information.

D-Link has now released firmware updates to address these two vulnerabilities with a number of affected devices, and pledged to release fixes for the remaining devices soon. If you are using a D-Link router, keep an eye out for updates as soon as new firmware arrives.