D-Link to issue router firmware updates for backdoor vulnerability

October 15 2013, by Nancy Owano

(Phys.org) —D-Link is tending to the router backdoor security issue that affects some of its routers. The company assures that it is "proactively working with the sources of these reports as well as continuing to review across the complete product line to ensure that the vulnerabilities discovered are addressed." The drama began on Saturday night, when it was discovered, thanks to Craig Heffner, a vulnerability researcher with

Tactical Network Solutions, that a backdoor-type function built into the firmware of some D-Link routers could be used to bypass standard authentication procedures. This was an opportunity to gain control of the device, potentially giving a criminal unauthorized access to a router's admin settings.

Heffner discovered the vulnerability in firmware. Once the authentication process was bypassed, one could change the router's settings. Heffner reported the issue. Word spread fast that a backdoor exploit opportunity had been found in a D-Link router's firmware code. Heffner, who worked on a D-Link DIR 100 to explore the vulnerability, explored further and said that, in total, seven different D-Link models of routers could be vulnerable.

Commenting on his discovery, the BBC noted that Heffner's analysis revealed a string of letters that, if used in a certain way, could unlock remote access. To see which other router models might have the same backdoor vulnerability, Heffner used a special search engine, Shodan. Heffner concluded that the same string could work on a total of seven D-Link router types, based on source code of the HTML pages and search results.

In response, D-Link stated that it is releasing firmware updates to address the vulnerability in affected routers. "Security and performance is of the utmost importance to D-Link across all product lines," D-Link said on its website.

D-Link is presently working with Heffner and other researchers to learn more about the vulnerability. D-Link said it is also continuing to review its entire product line to make sure vulnerabilities are addressed."We are proactively working with the sources of these reports," the company said in a statement.

As of the time of this writing, on its security page, D-Link already had posted a number of patches it was making available to address the vulnerability. The page is titled "Update on Router Security issue." The company said that "Various media reports have recently been published relating to vulnerabilities in network routers, including D-Link devices."

The company released firmware updates for the DIR-300, DIR-600, DIR-615, DIR-645, DIR-815, DIR-845L, DIR-865L, DSL-320B and DSL-321B.

"These firmware updates address the security vulnerabilities in affected D-Link routers," the page stated. "D-Link will update this continually and we strongly recommend all users to install the relevant updates."

The company also advised against responding to unsolicited e-mails related to security vulnerabilities prompting the user to take action.

"When you click on links in such e-mails, it could allow unauthorized persons to access your router. Neither D-Link nor its partners and resellers will send you unsolicited messages where you are asked to click or install something." D-Link also suggested disabling remote access to the router if it is not required.