Reported Vulnerability - D-Link routers authenticate administrative access using specific User-Agent string

Overview

Various D-Link routers allow administrative web actions if the HTTP request contains a specific User-Agent string. This backdoor allows an attacker to bypass password authentication and access the router's administrative web interface. Planex and Alpha Networks devices may also be affected, please contact these vendors directly at their regional websites.

Reference

US-Cert - VU# 248083 - http://bit.ly/17w4qzK
CVE-2013-026 - Craig Heffner - http://1.usa.gov/Ha5DG4
Craig Heffner, Tactical Network Solutions & Independent Security Professional - http://bit.ly/1bOtb1F

General Disclosure

Security and performance is of the utmost importance to D-Link across all product lines. This is not just through the development process but also through regular firmware updates to comply with the current safety and quality standards. We are 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. We will continue to update this page to include the relevant product firmware updates addressing these concerns. In the meantime, you can exercise the below cautions to avoid unwanted intrusion into your D-Link router.

Immediate Recommendations for all D-Link router customers

- Do not enable the *Remote Management* feature since this will allow malicious users to use this exploit from the Internet. *Remote Management* is default disabled on all D-Link Routers and is included for customer care troubleshooting if useful and the customer enables it.
- If you receive unsolicited e-mails that relates to security vulnerabilities and prompt you to action, please ignore it. 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.
- Make sure that your wireless network is secure.

Details

If device owner has enabled the '*Remote Management*' feature on the effected device, or malicious attacker has found a way to enable this feature. This exploit allows remote attackers to bypass authentication and modify settings via an xmlset_roodkcableoj28840ybtide User-Agent HTTP header. Should an effected device be exploited the user runs the risk of attacks present under CVE-2013-6027 (http://1.usa.gov/Ha5DG0) Stack-based Overflow which would cause the device to malfunction.

Effected Products

WW= Worldwide English Version - Used in North America CN=China EU=Europe FR=France
DE=Germany KR=Korea TW=Taiwan RU=Russia

Model Name	HW Version	Current FW Version	New FW Version for this exploit fix
DIR-100	A1	1.13	1.14B01 (WW) 1.14 Regional (CN, EU, FR, DE, KR, TW)
DIR-120	A1	1.03 1.04RU	1.05B01 (WW) 1.05RUB01 (RU)
DI-524	E3/E4	5.12	5.13B01 (WW)
DI-524UP	A1/A2	1.07	1.08B01 (WW)
DI-624S	B1/B2	1.11	1.12B01 (WW) 1.12 Regional (TW)
DI-604UP	A1	1.03	1.04B01 (WW)
DI-604+	A1	1.10	1.11B02 (WW)
TM-G5240	A1	4.00B29	4.01B01 (WW)

Security patch for your D-Link router

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

As there are different hardware revisions on our products, please check this on your device before downloading the correct corresponding firmware update. The hardware revision information can usually be found on the product label on the underside of the product next to the serial number. Alternatively, they can also be found on the device web configuration.

Thank You,

D-Link Customer Care