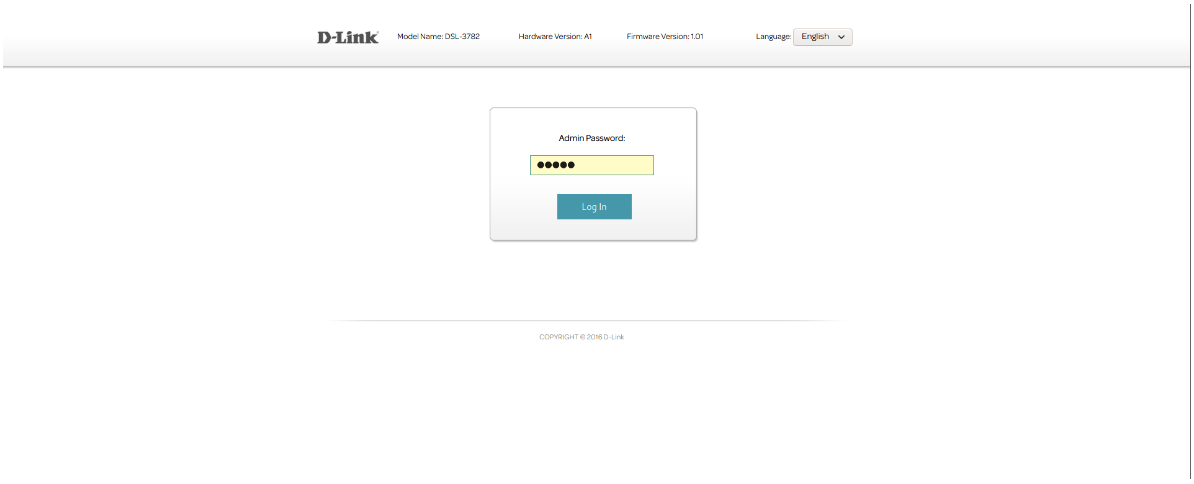
Some vulnerabilities (including a stack-based buffer overflow and a command injection) exist in the D-Link DSL-3782 Wi-Fi router 1.01 and 1.03.

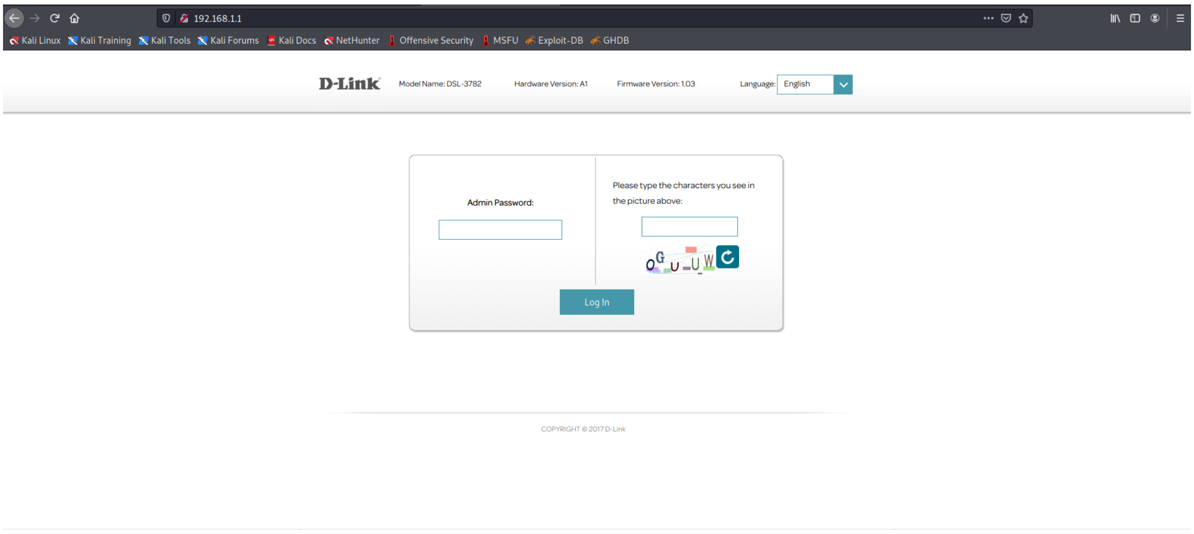
1. Command injection
   - In the codes which are used to perform the *Diagnostics* function of the cfg_manager program, the sprintf method uses the parameter from the web requests. The attackers can construct a payload to carry out arbitrary code attacks. To bypass the filter method, attackers can use the "%0a" as the delimiter.
2. Stack-based buffer overflow
   - In the getAttrValue function of the cfg_manager program, the strcpy method directly uses the service parameter from the tcapi program. The attackers can construct a payload to carry out arbitrary code attacks.



Model Name: DSL-3782 Hardware Version: A1 Firmware Version: 1.01 Language: English

Admin Password: ●●●●●

COPYRIGHT © 2016 D-Link



192.168.1.1

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Model Name: DSL-3782 Hardware Version: A1 Firmware Version: 1.03 Language: English

Admin Password:

Please type the characters you see in the picture above:

COPYRIGHT © 2017 D-Link