DD-WRT Information Disclosure Vulnerability

Craig Heffner
www.devttys0.com

Vulnerability Summary

Remote attackers can gain sensitive information about a DD-WRT router and internal clients, including IP addresses, MAC addresses and host names. This information can be used for further network attacks as well as very accurate geolocation. This is exploitable even if remote administration is disabled.

Affected Products

The vulnerability has been tested and confirmed in the following DD-WRT firmware:

- v24-preSP2 build 14896
- v24-preSP2 build 14311

Other versions may also be affected.

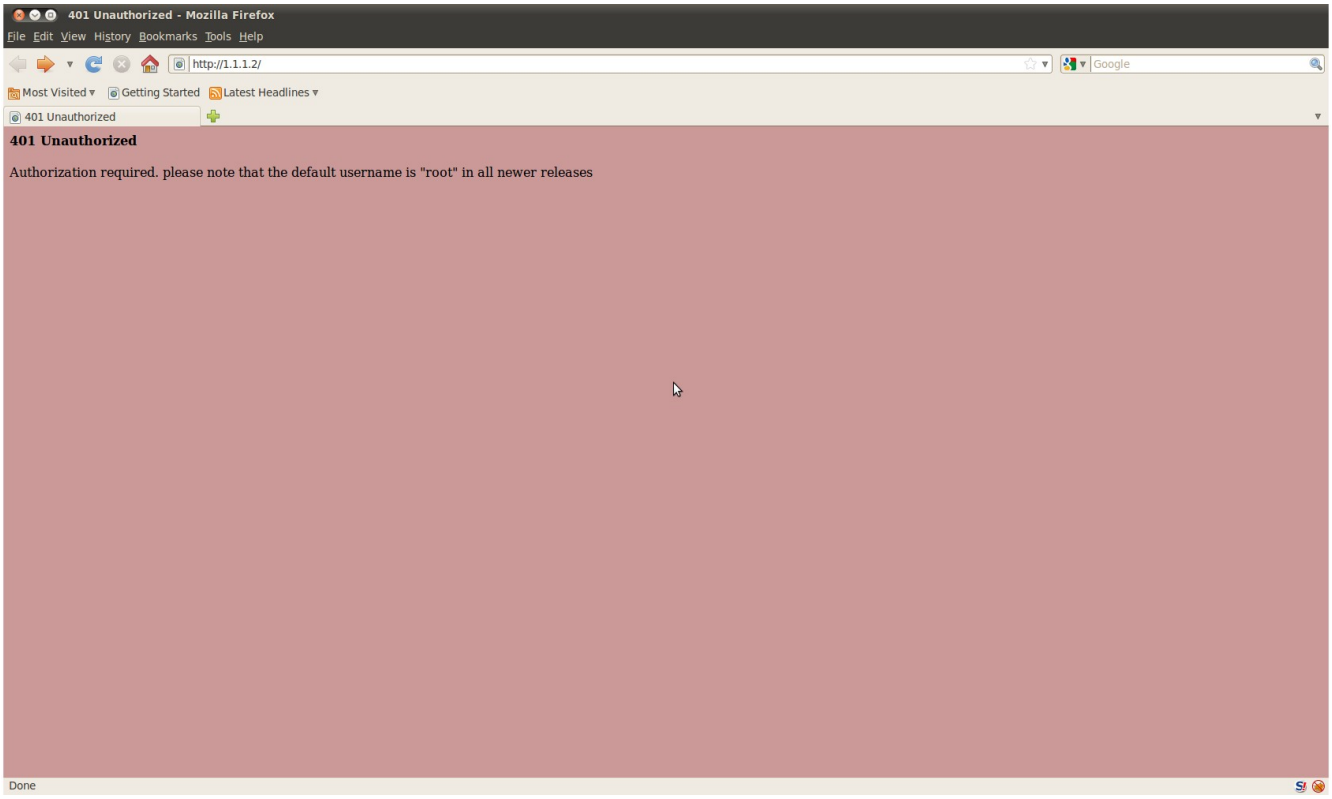
Vulnerability Description

The DD-WRT Web administration info page by default displays various statistics related to the router and internal network. This page can be configured to one of three settings: 'enabled', 'disabled', or 'enabled with password protection'. The default is 'enabled', which allows users to view the info page without authentication.

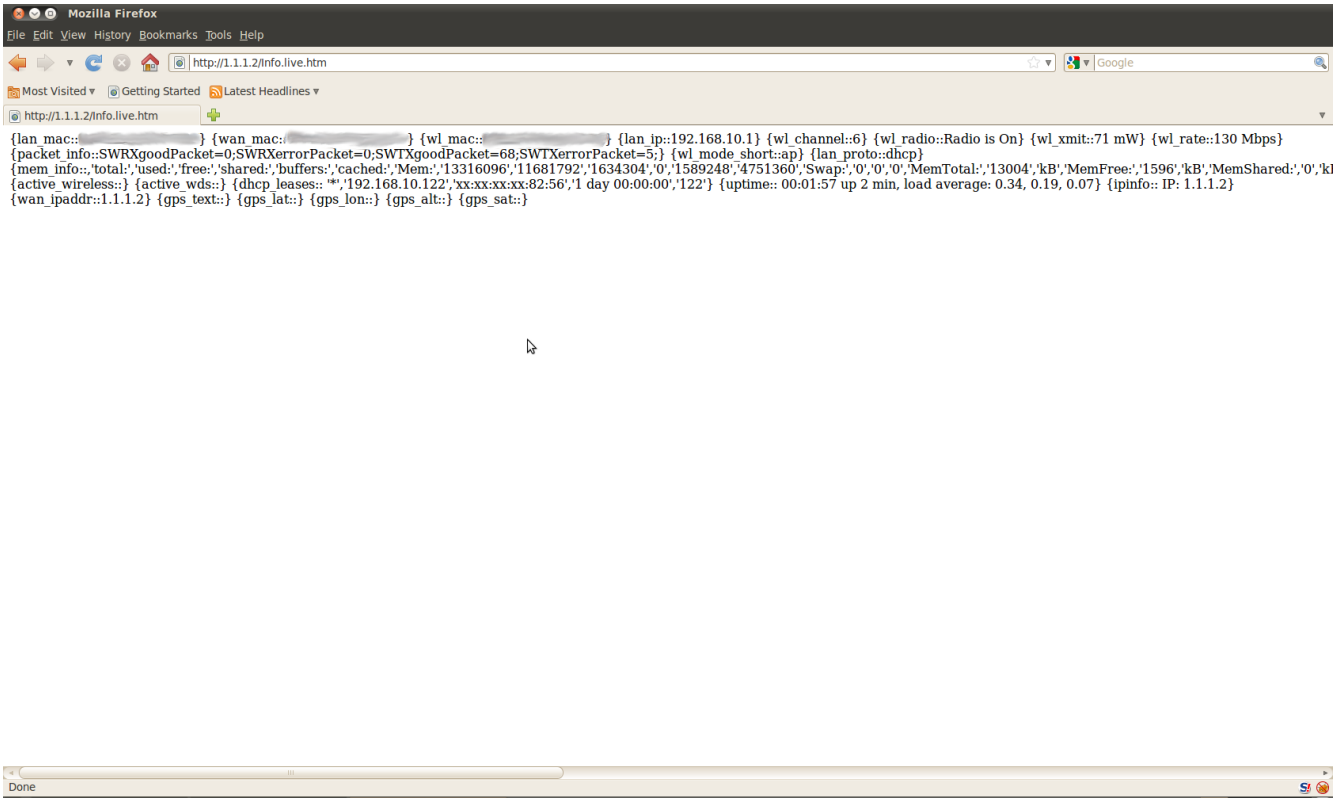
The info page is updated in real time via Javascript requests to /Info.live.htm. The /Info.live.htm page returns the following data (emphasis added, formatted for readability):

{lan_mac::00:22:B0:9B:1C:D3}
{wan_mac::00:22:B0:9B:1C:D4}
{**wl_mac::00:22:B0:9B:1C:D5**}
{**lan_ip::192.168.1.1**}
{wl_channel::6}
{wl_radio::Radio is On}
{wl_xmit::71 mW}
{wl_rate::270 Mbps}
{packet_info::SWRXgoodPacket=0;SWRXerrorPacket=0;SWTXgoodPacket=302;SWTXerror Packet=17;}
{wl_mode_short::ap}
{lan_proto::dhcp}
{mem_info::,'total:','used:','free:','shared:','buffers:','cached:','Mem:','13316096','11509760','1806336','0','1556480','4431872','Swap:','0','0','0','MemTotal:','13004','kB','MemFree:','1764','kB','MemShared:','0','kB','Buffers:','1520','kB','Cached:','4328','kB','SwapCached:','0','kB','Active:','4136','kB','Inactive:','1724','kB','HighTotal:','0','kB','HighFree:','0','kB','LowTotal:','13004','kB','LowFree:','1764','kB','SwapTotal:','0','kB','SwapFree:','0','kB'}
{active_wireless::}
{active_wds::}
{dhcp_leases:: **'joes-desktop','192.168.1.102'**,'xx:xx:xx:xx:2E:41','1 day 00:00:00','102'}
{dhcp_leases:: **'marys-laptop','192.168.1.105'**,'xx:xx:xx:xx:55:E2','1 day 00:00:00','105'}
{uptime:: 01:35:40 up 8 min, load average: 1.60, 0.80, 0.36}
{ipinfo:: IP: 1.1.1.1}
{wan_ipaddr::1.1.1.1}
{gps_text::}
{gps_lat::}
{gps_lon::}
{gps_alt::}
{gps_sat::}

For security, particularly when enabling remote administration, the info page configuration can be set to 'disabled', which will prevent unauthenticated users from viewing the router's info page:



However, unauthenticated users can still request the /Info.live.htm page directly and obtain sensitive network information:



Potential for Exploitation

Users who enable remote administration typically set the info page to 'disabled' or 'enabled with authentication' in order to prevent remote users from obtaining this information without first authenticating to the router. If the info page is disabled and remote administration is enabled, the /Info.live.htm page can still be accessed directly by an unauthenticated remote attacker.

Since DD-WRT is also vulnerable to a public IP DNS rebinding attack, this vulnerability affects routers that have remote administration disabled as well, and can be exploited by any Web site that is viewed by an internal, unauthenticated user [1]. The Rebind tool easily facilitates this type of rebinding attack [2, 5].

Regardless of the remote administration setting, if the info page is set to 'enabled' or 'disabled', remote attackers can obtain this information. Since the default setting is 'enabled', there is a high likelihood that the majority of DD-WRT installations are vulnerable to this attack.

Vulnerability Impact

This vulnerability can be used to gather information about a network for mounting a targeted attack.

Additionally, because a remote attacker can get the MAC address of the WLAN interface, the router's physical location can be very precisely identified via Google Location Services or Skyhook [3, 4].

Mitigations

This threat can be mitigated by setting the info page configuration to 'enabled with password protection'. In this configuration, all requests to /Info.live.htm must provide proper authentication.

Additional Information

A demonstration video has been created, depicting the Rebind tool being used to grab the contents of the /Info.live.htm page from a DD-WRT router that has both remote administration and the info page disabled. The router's wireless MAC address is then fed to Google Location Services to reveal the physical location of the device [5].

References

[1] https://media.blackhat.com/bh-us-10/whitepapers/Heffner/BlackHat-USA-2010-Heffner-How-to-Hack-Millions-of-Routers-wp.pdf

[2] http://rebind.googlecode.com

[3] http://samy.pl/mapxss/

[4] http://www.skyhookwireless.com/

[5] http://www.youtube.com/watch?v=7sd2mhq2ILQ