Willgues Security Blog

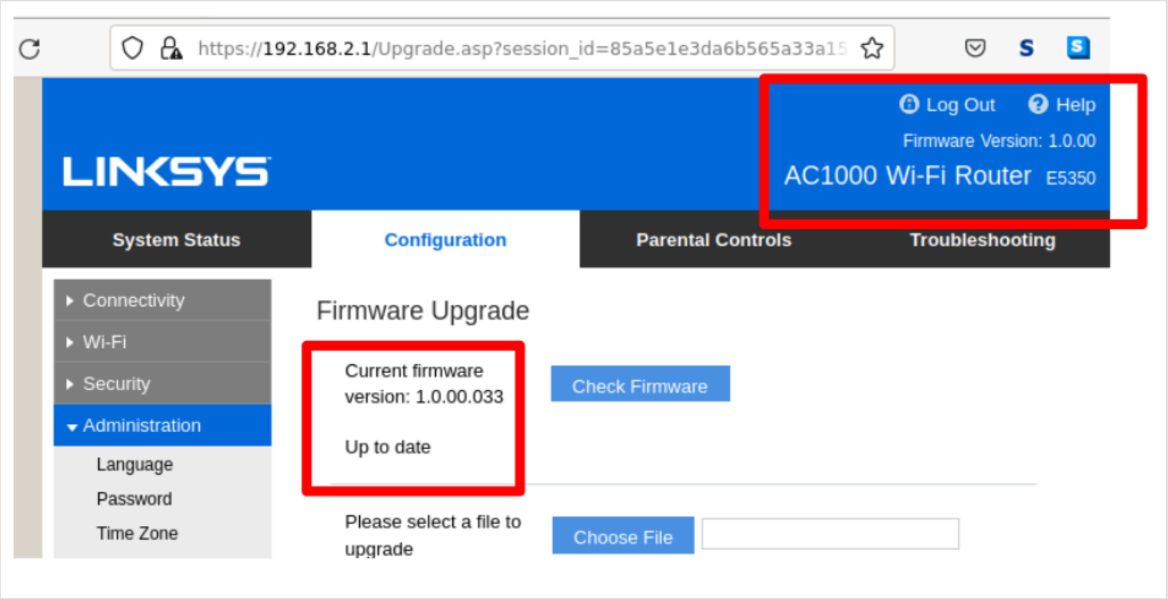
Linksys E5350 Password Disclosure Vulnerability (CVE-2022-35572)

Posted on **July 7, 2022**

Affected Products: Linksys E5350 AC1000 WiFi Router (Possibly More Models)
Affected Versions: 1.0.00.037 and lower
Vulnerability Type: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Description: The SysInfo.htm webpage on Linksys E5350 AC1000 WiFi routers versions 1.0.00.037 and lower exposes plaintext WPA2 passwords, MAC addresses, firmware versions, and other identifiers without authentication. If remote management is enabled, this vulnerability is exploitable remotely over the internet.

Recently, I began analyzing my Linksys E5350 WiFi router to see if I could find any vulnerabilities. I noticed that the firmware update mechanism supports an easy to use update mechanism, and employs a signed update, which was good. I found that I am running the most recent version of the firmware, 1.0.00.033 (note the vendor did push a newer version of the firmware in May 2022 after I wrote this, which does **not** remediate the issue, so FW version 1.0.00.037 is still vulnerable after testing)



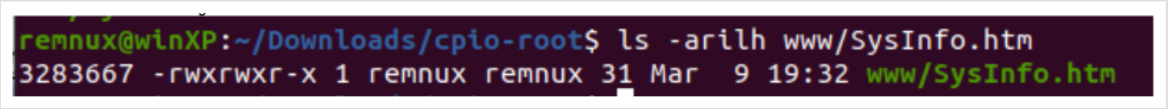
Firmware Upgrade

Current firmware version: 1.0.00.033

Up to date

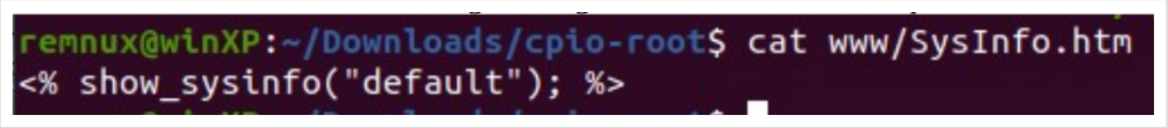
Please select a file to upgrade

I discovered some information disclosure vulnerabilities when I began searching for any files accessible via the router's httpd web server, specifically files that were not available to be accessed via normal browsing.
Using directory brute force tools like Gobuster or Dirbuster, or using firmware analysis will reveal SysInfo.htm:



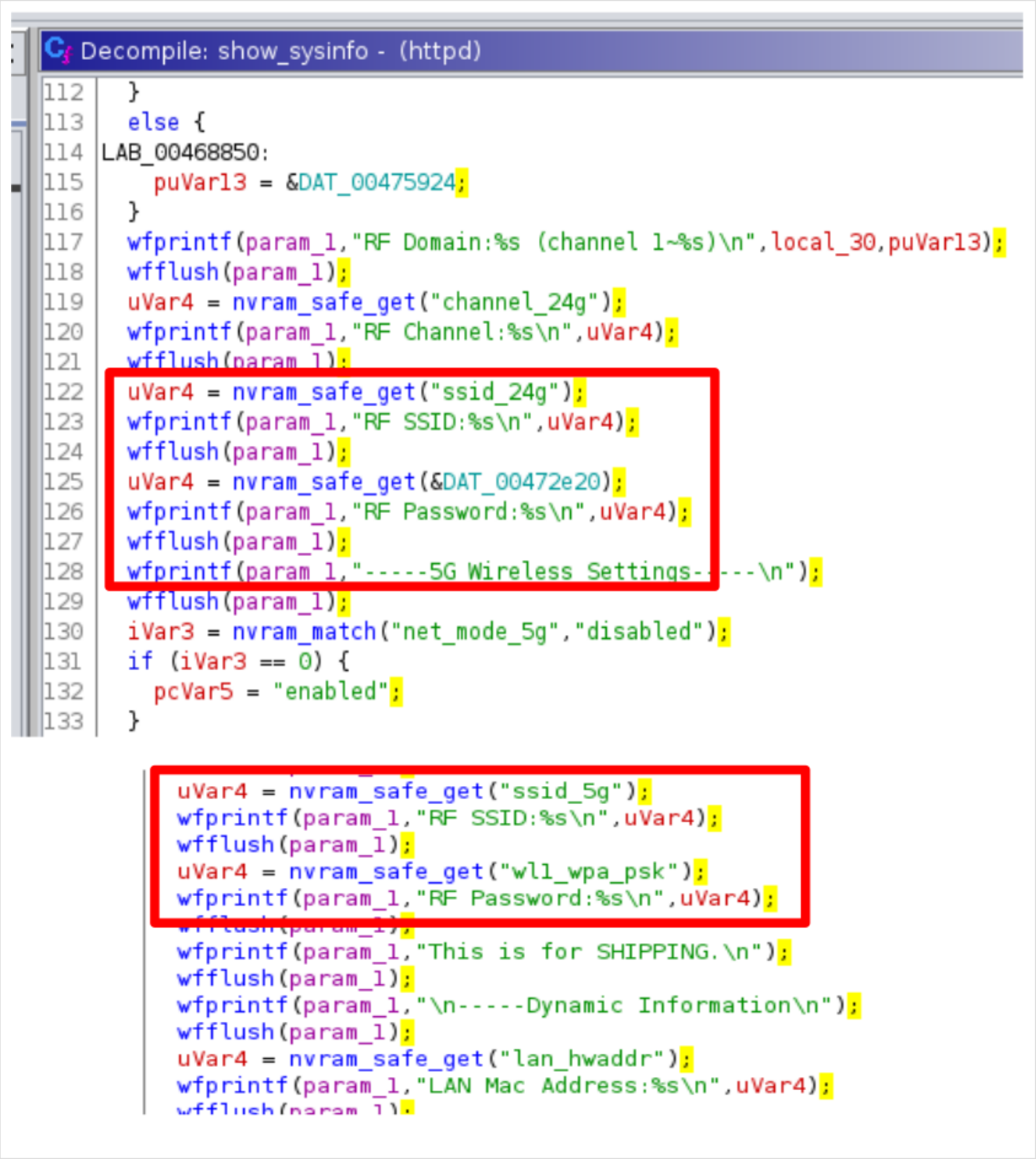
```
remnux@winXP:~/Downloads/cpio-root$ ls -arilh www/SysInfo.htm
3283667 -rwxrwxr-x 1 remnux remnux 31 Mar  9 19:32 www/SysInfo.htm
```

We can view the source code of the document, and see that it does not require a session ID like the rest of the pages hosted on the router's httpd service. The file is only one line of code which calls an information gathering function, but **doesn't require a session ID**:



```
remnux@winXP:~/Downloads/cpio-root$ cat www/SysInfo.htm
<% show_sysinfo("default"); %>
```

After extracting the httpd binary, we can disassemble it using open source tools like Ghidra, viewing
the assembly code and a decent C representation. We can see show_sysinfo function extracts several bits of confidential information from the device without requiring authentication. Some examples of the data disclosed are WPA2 passwords, MAC Addresses, SSIDs, serial numbers, and so on:

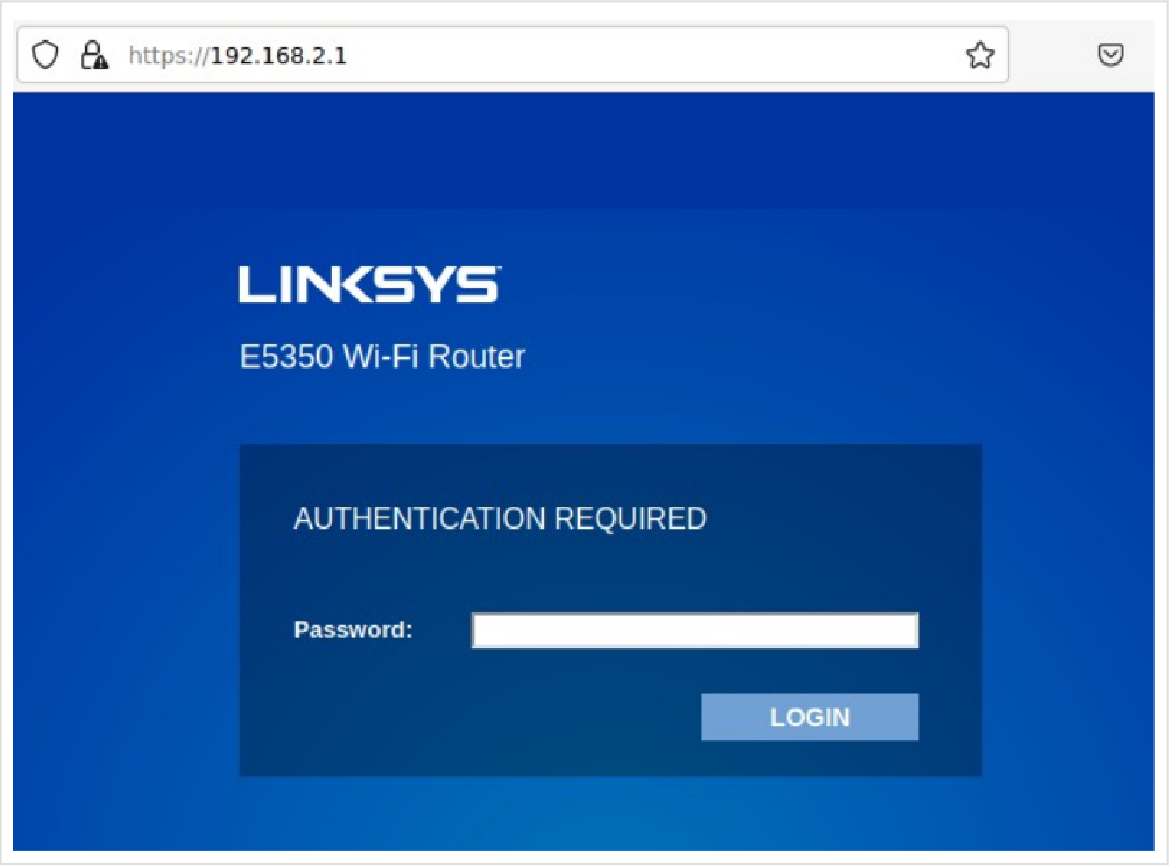


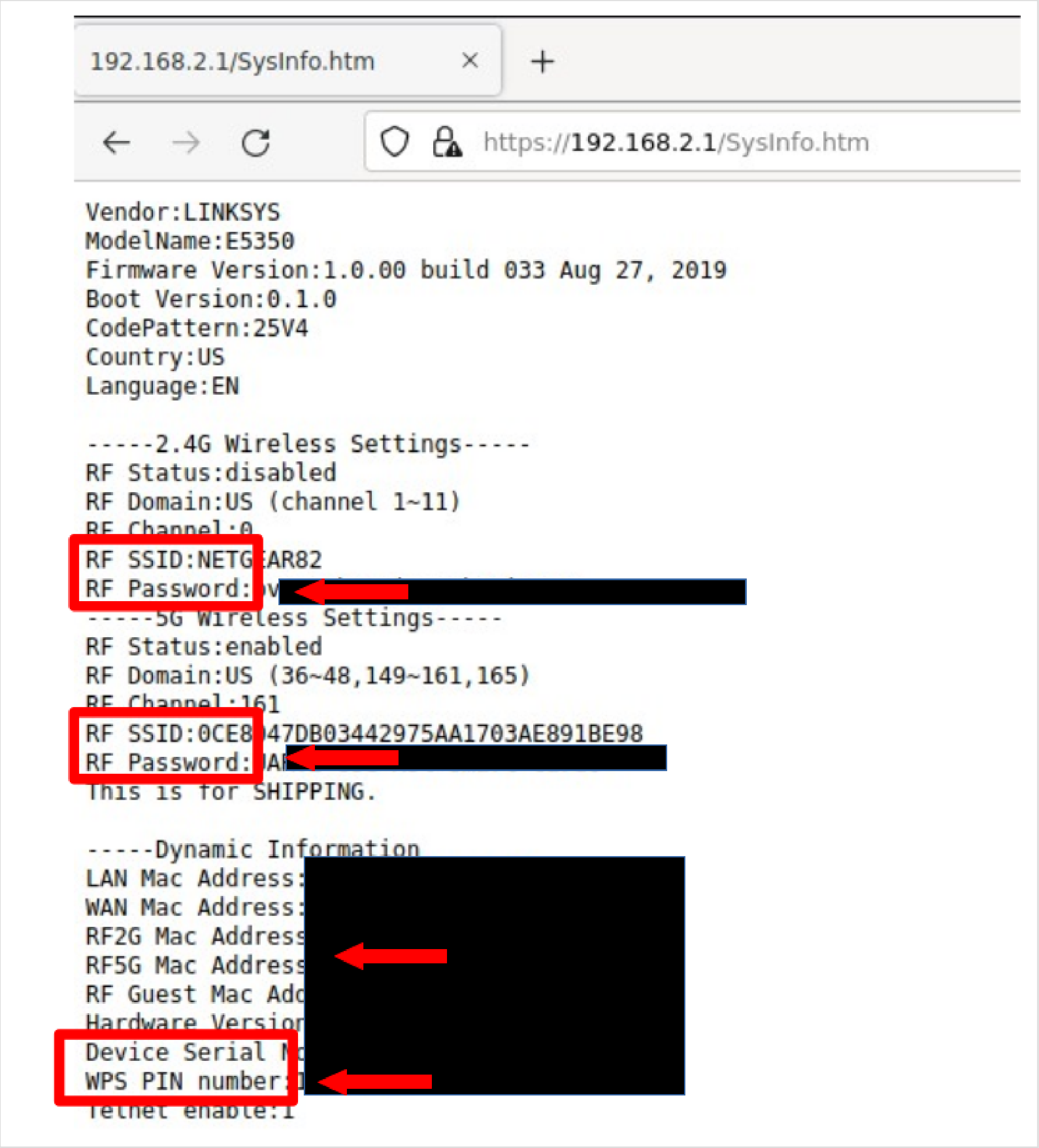
Decompile: show_sysinfo - (httpd)

```
  }
  else {
LAB_00468850:
    puVar13 = &DAT_00475924;
  }
  wfprintf(param_1,"RF Domain:%s (channel 1~%s)\n",local_30,puVar13);
  wfflush(param_1);
  uVar4 = nvram_safe_get("channel_24g");
  wfprintf(param_1,"RF Channel:%s\n",uVar4);
  wfflush(param_1);
  uVar4 = nvram_safe_get("ssid_24g");
  wfprintf(param_1,"RF SSID:%s\n",uVar4);
  wfflush(param_1);
  uVar4 = nvram_safe_get(&DAT_00472e20);
  wfprintf(param_1,"RF Password:%s\n",uVar4);
  wfflush(param_1);
  wfprintf(param_1,"-----5G Wireless Settings-----\n");
  wfflush(param_1);
  iVar3 = nvram_match("net_mode_5g","disabled");
  if (iVar3 == 0) {
    pcVar5 = "enabled";
  }
```

```
uVar4 = nvram_safe_get("ssid_5g");
wfprintf(param_1,"RF SSID:%s\n",uVar4);
wfflush(param_1);
uVar4 = nvram_safe_get("wl1_wpa_psk");
wfprintf(param_1,"RF Password:%s\n",uVar4);
wfflush(param_1);
wfprintf(param_1,"This is for SHIPPING.\n");
wfflush(param_1);
wfprintf(param_1,"\n-----Dynamic Information\n");
wfflush(param_1);
uVar4 = nvram_safe_get("lan_hwaddr");
wfprintf(param_1,"LAN Mac Address:%s\n",uVar4);
wfflush(param_1);
```

We can confirm this behavior by viewing the router with an empty session, and not logging in, and then trying to access the /SysInfo.htm URI:


https://192.168.2.1
LINKSYS
E5350 Wi-Fi Router
AUTHENTICATION REQUIRED
Password:
LOGIN



```
Vendor:LINKSYS
ModelName:E5350
Firmware Version:1.0.00 build 033 Aug 27, 2019
Boot Version:0.1.0
CodePattern:25V4
Country:US
Language:EN

-----2.4G Wireless Settings-----
RF Status:disabled
RF Domain:US (channel 1~11)
RF Channel:0
RF SSID:NETGEAR82
RF Password:[redacted]
-----5G Wireless Settings-----
RF Status:enabled
RF Domain:US (36~48,149~161,165)
RF Channel:161
RF SSID:0CE8047DB03442975AA1703AE891BE98
RF Password:[redacted]
This is for SHIPPING.

-----Dynamic Information
LAN Mac Address:[redacted]
WAN Mac Address:
RF2G Mac Address
RF5G Mac Address
RF Guest Mac Add
Hardware Versior
Device Serial N
WPS PIN number:
Telnet enable:1
```

Note that the Passwords and other confidential information has been covered, but the WPA passwords are displayed in plaintext, as well as all MAC addresses in use on the device.

We can see that this page does not require authentication, exposing information about the device which should be restricted to authenticated users only, including cryptographic secrets (WPA2 passwords). A user may only be granted access to the 2.4 ghz network, but now have the password for the 5GhZ. The WPS Pin number is also exposed.

I noticed during my analysis that this device has an option to disable firmware upgrades over remote management. Therefore, I decided to test if this vulnerability is also present when the httpd service is exposed over a WAN connection (internet facing), which increases the impact of the vulnerability. Note in the earlier screenshots the 192.168.2.1 IP range, this is the LAN side of the WiFi router.

Connecting from the WAN side in the 10.x range, as the 10.x IP address is assigned to the WiFi router via a Firewall DHCP server.

Now, we can test the /SysInfo.htm URI again and see if it works:

This vulnerability allows a threat actor with the ability to connect to the remote management interface (over the internet) to harvest the WPA passwords, MAC Addresses, serial numbers, and software versions of the device without authentication. The exposed passwords could also be used to gain access to the administrator interface. The unique identifiers that are leaked allow tracking of users that are using these routers.

Since the MAC Address of the wireless card is leaked, a threat actor could correlate data gathered from this vulnerability with WiFi Access Point mapping services and pinpoint the physical location of a device they enumerated over the internet.

Due to the popularity of the router, as well as the commonality of remote management by advanced users, this likely exposes tens of thousands of routers to password disclosure. Using open source websites like Shodan I was able to confirm over 1000 devices similar to mine located in the United States which have a unique string in the HTTP request that allows them to be fingerprinted.

Additionally, I found that when setting up remote management, HTTP is checked by default instead of HTTPS. This means the majority of administrators will unknowingly lessen the security.

Hardcoded Linksys Telnet Password

In addition to the previous information disclosure vulnerability, I was able to discover that all of these devices use the same hard coded telnet password.

To preface, telnet is disabled by default, so this issue would only affect users which have enabled telnet.

A hidden menu, System.asp, has very useful info about the device which does not compromise security, and was nice to see that Linksys included it. Please note the System.asp menu does require authentication, and it provides all the information available via SysInfo.htm. An easy resolution to the SysInfo.htm vulnerability is simply to delete the file and push a firmware update.

Inside the System.asp menu, there is a button to enable/disable telnet. However, once telnet is enabled, the credentials for the web admin interface are not accepted, and I could not find credentials on the internet.

Using a simple grep statement to search the filesystem, we find a credential for an account named “root”:

Now, we can enable telnet at the System.asp menu:

Now we can connect to the device using telnet, and observe we obtain a root shell using the obtained credentials:

This becomes an issue if an advanced user has enabled telnet, but did not disable it, and anyone can now connect as root to the router and cause damage or infect the device.

Additionally, we can observe the same telnet credentials in a configuration backup file accessible via the Web Interface (config backup option):

A way to resolve this issue is to randomize the root password for every device, so an advanced or authorized user can enable and access telnet if they wish, but then all devices will have a unique password, mitigating any knowledge of the “cbt4blk” password.

I will put out another article that details my explorations of this device as far as non-security related findings go.

It appears this device has shared code with many other routers / IOT devices, so other devices may also may be vulnerable. I used the following article as a reference, which describes finding many vulnerabilities in Cisco ATA phone adapters, and I could notice shared code between the two devices (although the vulnerabilities from the article were patched for this device):

https://medium.com/tenable-techblog/rce-in-cisco-voip-adapters-115784b6d32b

I attempted to contact Linksys via their bug bounty program on bugcrowd and submitted this vulnerability in March 2022. As of July 7 2022, the report has not been acknowledged or responded to in any way by Linksys even after multiple attempts to reach out.

This entry was posted in **Uncategorized** by **willgues**. Bookmark the **permalink [https://willgu.es/?p=76]** .