The Linksys smart Wi-Fi router was found to contain information leaks of connected devices

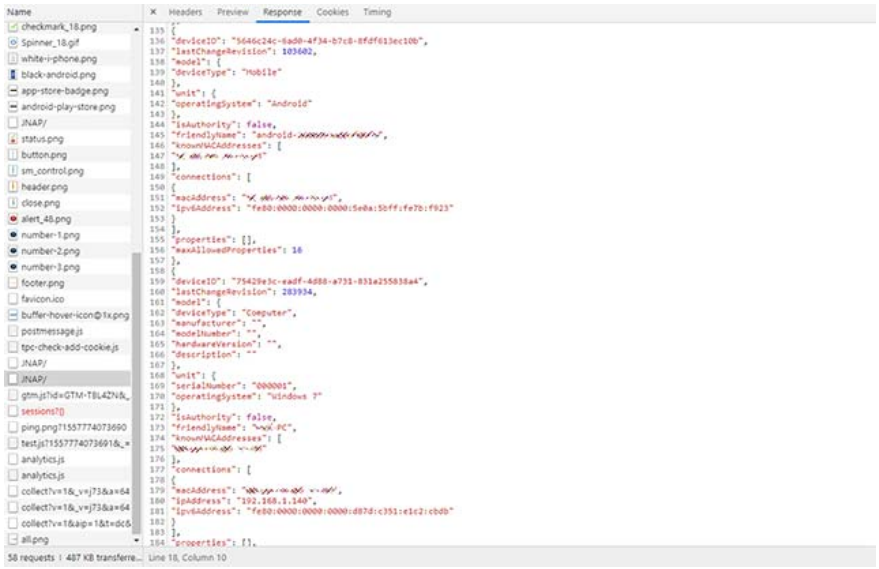
More than 25,000 smart Wi-Fi router devices (smart Wi-Fi routers) with Linksys famous brands are said to be affected by a serious security hole.

More than 25,000 smart Wi-Fi router devices (smart Wi-Fi routers) with Linksys famous brands are said to be affected by a serious security vulnerability, thereby disclosing information as well as giving allows remote and unauthenticated access to a wide range of sensitive data about connected devices.

This issue is generally very similar to the Linksys SMART WiFi software security problem that has appeared since 2014, followed by the CVE-2014-8244 identifier, allowing "remote attackers to steal information." sensitive or modify data through JNAP operations in JNAP / HTTP requests ".

1. UC Browser Android - lucrative bait for URL spoofing attacks

However, according to a report by security researchers from the Bad Packet organization headed by computer forensic expert Troy Mursch, although it is thought to have been successfully patched about 5 years ago, but the result left by CVE-2014-8244 is still there, and directly affects Linksys devices as mentioned above. More blameless, Linksys did not offer any security recommendations to users or any patching action. Worse, the Linksys security team tagged the Troy Mursch vulnerability report as "Not applicable / Won't fix" and closed the topic.



1. More than 4,000 Office 365 accounts are affected by account hijacking attacks

Back to Troy Mursch's report. He and his colleagues discovered that 25,617 Linksys smart Wi-Fi router products contained vulnerabilities that made them vulnerable to security attacks, and could expose a range of sensitive information. feel of connected devices such as:

1. The MAC address of every device that has been connected to it (full history record of all connected devices, not just active devices).
2. Device name (such as 'QUANTRIMANG-PC' or 'My MacBook Pro').
3. The operating system the device is using (such as Windows 7, Windows 10 or Android .).
4. WAN settings, firewall status, firmware update settings and DDNS settings.
5. Additional metadata is recorded as device type, model number and detailed description of the device.

More seriously, leaked sensitive information can be accessed easily by opening the login interface of the Linksys Smart Wi-Fi router that contains this security hole in the web browser, and then Just click on the JNAP requests in the left bar.

Besides, Troy Mursch also stated in his report that "this vulnerability could allow disclosure of sensitive information without authentication and could be exploited by an amateur attacker, yes. little technical knowledge ".

Model Number	Description
E1200	Linksys E1200
E4200	Simultaneous Dual-Band Wireless-N Gigabit Router
EA2700	Simultaneous Dual-Band Wireless-N Gigabit Router
EA2750	Simultaneous Dual-Band Wireless-N Gigabit Router
EA3500	Simultaneous Dual-Band Wireless-N Gigabit Router
EA4500	Simultaneous Dual-Band Wireless-N Gigabit Router
EA5800	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6100	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6200	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6300	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6350	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6400	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6500	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6700	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA6900	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA7300	Max-Stream AC1750 MU-MIMO GIGABIT ROUTER
EA7400	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA7500	Max-Stream AC1900 MU-MIMO GIGABIT ROUTER
EA8100	Max-Stream AC2600 MU-MIMO GIGABIT ROUTER
EA8300	Linksys AC2200 MU-MIMO Gigabit Tri-Band Router
EA8500	Simultaneous Dual-Band Wireless-AC Gigabit Router
EA9200	Linksys AC3200 Tri-Band Smart Wi-Fi Router
EA9300	Linksys MAX-STREAM AC4000 MU-MIMO Tri-Band Router
EA9400	Linksys MAX-STREAM AC5000 MU-MIMO Gigabit Router
EA9500	Linksys MAX-STREAM AC5400 MU-MIMO Gigabit Router
WRT1200AC	Simultaneous Dual-Band Wireless-AC Gigabit Router
WRT1900AC	Simultaneous Dual-Band Wireless-AC Gigabit Router
WRT1900ACS	Simultaneous Dual-Band Wireless-AC Gigabit Router
WRT3200ACM	Simultaneous Dual-Band Wireless-AC Gigabit Router
XAC1200	Simultaneous Dual-Band Wireless-AC Gigabit Router
XAC1900	Simultaneous Dual-Band Wireless-AC Gigabit Router

1. Dell computers became victims of RCE attacks by vulnerabilities in SupportAssist

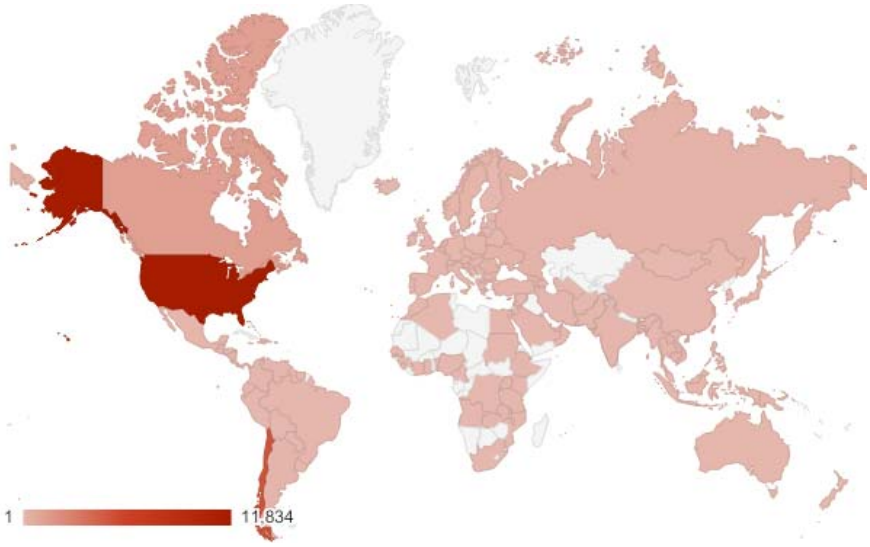
The team found Wi-Fi smart routers of vulnerable Linksys being used in 146 countries, on the network of 1998 internet service providers, with 11,834 of them discovered in the United States. States, 4,942 in Chile, 2,068 in Singapore and 1,215 in Canada.

For the rest of the country, the number of vulnerable Wi-Fi Linksys smart routers is now accessible from the internet, not much, mostly at less than 500 devices, including: 462 in Hong Kong, 440 in the United Arab Emirates, 280 in Qatar, 255 Russia, 225 in Nicaragua and 203 in the Netherlands. 3,723 other devices are scattered in the remaining countries in negligible quantities.

In addition, Troy Mursch's team has discovered thousands of Linksys smart Wi-Fi routers that are using default admin passwords and can easily be accessed by potential attackers as well. like instant access.

When a cybercrime has control of one of these routers, they will be able to perform the following malicious behaviors:

1. Steal SSID and Wi-Fi passwords as plain text.
2. Change DNS settings to use a fake DNS server to thereby control web traffic.
3. Open ports in the router's firewall to target devices directly behind that router (eg 3389 / tcp for Windows RDP).
4. Use UPnP to redirect traffic to an attacker's device.
5. Create an OpenVPN account (supported models) to route malicious traffic through hijacked routers.
6. Disable the internet connection of the router or modify other installation modes for destructive purposes.



1. Malware stored in Google Sites sends data to the MySQL server

However, Mr Troy Mursch also said that although Linksys security team moves showed that at the moment they are trying to avoid the need to overcome the security vulnerability extremely dangerous on real estate. products, but the company "has enabled the firmware update feature automatically". This means Linksys will sooner or later fix this vulnerability. Devices on the list containing vulnerabilities will receive security updates as well as being placed under automatic protection processes. Linksys's silence at the moment is probably because the company still cannot find the best response method for this vulnerability.

So, if you own any Linksys Wi-Fi smart router device, it is better to stop using it for a while, at least until the Linksys side releases the patch. can. On the other hand, all current updates do not work in this case because they do not come with vulnerability patches.

1. Discover Dragonblood security vulnerability in WPA3

In addition, "disabling remote web access will not be a good option as all Linksys Wi-Fi routers will require remote web access, the Linksys app comes with can work ".