Hundreds of thousands of Wifi manufactured from 2015 and earlier were attacked

If you are using a Wifi router, Wifi extender or USB Wifi made in 2015 or earlier, it may be time to ditch it and buy a new one. Because your device is too old and can be hacked over the Internet now.

Critical vulnerabilities have been found in hundreds of Wi-Fi models for home use. They are manufactured and sold by 65 different companies and are under attack. The list of hacked models is listed at the bottom of the page.

Many of the hacked models were manufactured between 2010 and 2015, with at least a few manufactured in 2004. IoT Inspector, a German information security company, discovered hundreds of thousands of vulnerable personal devices worldwide.

"By exploiting these vulnerabilities, remote unauthenticated attackers can fully compromise the device and execute arbitrary code with the highest level of privileges," IoT Inspector said.

In the IoT Inspector report published on August 16, a criminal gang attacked these devices.

Israeli information security company SAM Seamless Network said it took just two days for botnet operators to use a variant of the notorious Mirai malware. On an October 2016 afternoon, that variant brought down Internet access in much of the US East Coast and began carrying out the attack.

The botnet gang is exploiting a specific vulnerability related to remote router takeover via the admin interface. Even disabling remote access cannot fix this problem.

Just accessing a malicious website on a computer with a router puts the user at risk. In addition, there are three other critical vulnerabilities.

These vulnerable devices all use Wifi chips manufactured by Realtek Company (Taiwan). In May, IoT Inspector informed Realtek of this vulnerability. On August 13, the company released patches for some Wi-Fi with vulnerable chipsets. Realtek is expected to roll out more patches, but has no plans to patch the oldest chipsets.

However, those patches must be made and tweaked by the vulnerable device manufacturers and then made available to users as new firmware.

Having patches available to download or install is less likely, and it may take several months before all firmware updates become available. The oldest devices will probably never receive the patch.

What to do when your Wifi on the list is attacked?

If the Wifi is only a few years old, say 2015 or later: You will probably receive a firmware update in the next few months.

Check the manufacturer's website now for updates released after August 13, 2021. See a firmware release that notes the vulnerability ID numbers CVE-2021-35392, CVE-2021 -35393, CVE-2021-35394 or CVE-2021-35395 or not. If so, contact Realtek or IoT Insprctor for assistance in locating the error.

Follow the instructions on the manufacturer's website to download and install the firmware.

If an update is not available, disconnect the device and use another router or access point until a firmware update is available.

If the device was manufactured between 2010 and 2015: You may or may not receive a firmware update. You do the same as above: Check the manufacturer's website for available firmware updates and follow the instructions.

If there is no new release as of August 13, 2021, disconnect the device and keep checking the site for the next few months.

If the device was first manufactured before 2010: You will probably never receive the firmware update, so you should buy a new Wifi.

List of hacked Wifi

Producer	Model	Producer	Model
A-Link Europe Ltd	A-Link WNAP WNAP(b)	beeline	Smart Box v1
ARRIS Group, Inc	VAP4402_CALA	Askey	AP5100W
Airlive Corp.	WN-250R, WN-350R	DASAN Networks	H150N
Abocom Systems Inc.	Wireless Router	Calix Inc.	804Mesh
AIgital	Wifi Range Extenders	China Mobile Communication Corp.	AN1202L
Amped Wireless	AP20000G	Compal Broadband Networks, INC.	CH66xx cable modems line.
Belkin	F9K1015, AC1200DB Wireless Router F9K1113 v4, AC1200FE Wireless Router F9K1123, AC750 Wireless Router F9K1116, N300WRX, N600DB	D-Link	DIR-XXX models based on rlx-linux, DAP-XXX models based on rlx-linux, DIR-300, DIR-501, DIR-600L, DIR-605C, DIR-605L, DIR-615, DIR-618, DIR- 618b, DIR-619, DIR-619L, DIR-809, DIR-813, DIR-815, DIR-820L, DIR-825, DIR-825AC, DIR-825ACG1, DIR-842, DAP-1155, DAP-1155 A1 , DAP-1360 C1, DAP-1360 B1, DSL-2640U, DSL-2750U, DSL_2640U, VoIP Router DVG-2102S, VoIP Router DVG-5004S, VoIP Router DVG-N5402GF, VoIP Router DVG-N5402SP, VoIP Router DVG-N5412SP , Wireless VoIP Device DVG-N5402SP
ASUSTek Computer Inc.	RT-Nxx models, WL330-NUL, Wireless WPS Router RT-N10E, Wireless WPS Router RT-N10LX, Wireless WPS Router RT-N12E, Wireless WPS Router RT-N12LX	Buffalo Inc.	WEX-1166DHP2, WEX-1166DHPS, WEX-300HPS, WEX-733DHPS, WMR-433, WSR-1166DHP3, WSR-1166DHP4, WSR-1166DHPL, WSR-1166DHPL2
BEST ONE TECHNOLOGY	AP-BNC-800	Davolink Inc.	DVW2700 1, DVW2700L 1

LG	Axler Router LGI-R104N, Axler Router LGI-R104T, Axler Router LGI-X501, Axler Router LGI-X502, Axler Router LGI-X503, Axler Router LGI-X601, Axler Router LGI-X602, Axler Router RT-DSE	Edimax	RE-7438, BR6478N, Wireless Router BR-6428nS, N150 Wireless Router BR6228GNS, N300 Wireless Router BR6428NS, BR-6228nS/nC
Edison		EnGenius Technologies, Inc.	11N Wireless Router, Wireless AP Router
ELECOM	WRC-1467GHBK, WRC-1900GHBK, WRC-300FEBK-A, WRC-733FEBK-A	Esson	Wifi Module ESM8196
EZ-NET Ubiquitous Corp.	NEXT-7004N	FIDA	PRN3005L D5
Hama		IO DATA	WN-AC1167R, WN-G300GR
Hawking Technologies	AWNR3	iCotera	i6800
MT-Link	MT-WR600N	Edge-core	VoIP Router ECG4510-05E-R01
LINK-NET	LW-N664R2, LW-U31, LW-U700	Logitec	R6428GNS, LAN-W300N3L
IGD	1T1L	MMC	MM01-005H, MM02-005H
MT-Link	MT-WR730N, MT-WR760N, MT-WR761N, MT-WR761N+, MT-WR860N	Nexxt Solutions	AEIEL304A1, AEIEL304U2, ARNEL304U1
NetComm Wireless	NF15ACV	Observa Telecom	RTA01
Netis	WF2411, WF2411I, WF2411R, WF2419, WF2419I, WF2419R, WF2681	Occtel	VoIP Router ODC201AC, VoIP Router OGC200W, VoIP Router ONC200W, VoIP Router SP300-DS, VoIP Router SP5220SO, VoIP Router SP5220SP
Netgear	N300R	Omega Technology	Wireless N Router O31 OWLR151U, Wireless N Router O70 OWLR307U

PATECH	Axler RT-TSE, Axler Router R104, Axler Router R3, Axler Router X503, Axler Router X603, LotteMart Router 104L, LotteMart Router 502L, LotteMart Router 503L, Router P104S, Router P501	PLANEX COMMUNICATIONS INC., Planex Communications Corp.	MZK-MF300N, MZK-MR150, MZK-W300NH3, MZK-W300NR, MZK-WNHR
PLANET Technology	Sitecom Wireless Gigabit Router WLR-4001, Sitecom Wireless Router 150N X1 150N, Sitecom Wireless Router 300N X2 300N, Sitecom Wireless Router 300N X3 300N	Realtek	RTL8196C EV-2009-02-06, RTL8xxx EV-2009-02-06, RTL8xxx EV-2010-09-20, RTL8186 EV-2006-07-27, RTL8671 EV-2006-07-27, RTL8671 EV-2010-09-20, RTL8xxx EV-2006-07-27, RTL8xxx EV-2009-02-06, RTL8xxx EV-2010-09-20
Revogi Systems		Sitecom Europe BV	VIP-281SV
Skystation	CWR-GN150S	Shaghal Ltd.	ERACN300
Sercomm Corp.	Telmex Infinitum	Shenzhen Yichen (JCG) Technology Development Co., Ltd.	JYR-N490
Skyworth Digital Technology.	Mesh Router	Smartlink	
Technicolor	TD5137	TCL Communication	
Telewell	TW-EAV510	Tenda	AC6, AC10, W6, W9, i21
Totolink	A300R		
TRENDnet, Inc., TRENDnet Technology, Corp.	TEW-651BR, TEW-637AP, TEW-638APB, TEW-831DR	UPVEL	UR-315BN
ZTE	MF253V, MF910	Zyxel	P-330W, X150N, NBG-2105, NBG-416N AP Router, NBG-418N AP Router, WAP6804