Securing IoT Devices:
How Safe Is Your Wi-Fi Router?

To date, many low-cost Internet-of-Things (IoT) devices lack adequate security provisions. As a result, U.S. households have a cluster of networked, electronic devices that offer vulnerable targets to hackers, such as digital cameras embedded in baby monitors, storage and computing devices, and sensors implanted in appliances. This ConsumerGram analyzes Wi-Fi routers and finds that 5 of every 6 routers are inadequately updated for known security flaws, leaving connected devices open to cyberattacks that can compromise consumer privacy and lead to financial loss.

A Vulnerable Source for Cyberattacks

The security of the software in the digital devices we use has a bearing on our privacy. For many of us, electronic devices like laptops and smartphones contain the record of our interactions with others, passwords, financial information, social media conversations, and other sensitive information. At a societal level, electronic devices and software are at the center of many of our day-to-day activities – employment, health records, entertainment and shopping – just to name a few. In addition, the security of digital computing and communications is essential to the operations of commerce, as well as our country's infrastructure and national security.

In May 2018, the FBI sent out a warning that Russian computer hackers had compromised hundreds of thousands of home and office routers and could collect user information or shut down network traffic.[1] They urged the owners of many brands of routers to turn them off and on again, and then download firmware updates from the manufacturers to

[1] Joseph Menn and Sarah N. Lynch, "FBI Warns Russians Hacked Hundreds of Thousands of Routers," *Reuters*, May 25, 2018, https://ca.news.yahoo.com/fbi-says-foreign-hackers-compromised-home-router-devices-155414530.html.

protect themselves. Earlier, Cisco warned that hackers were targeting popular routers made by Linksys, NETGEAR, TP-Link, and others.[2]

Hackers target hardware devices such as routers because they are usually left on and their accompanying software, called *firmware*, are infrequently updated.[3] Firmware is more and more frequently built on open source code, which is, as many believe, to be more prone to hacking.[4] The use of open source code as a cost-effective way to allow customization has grown across all industries in recent years. Open source is now everywhere, including operating systems, applications software, development tools, and routers. As vulnerabilities are found in open source code, the numerous router manufacturers may or may not take the necessary steps to patch these vulnerabilities when fixes become available.

Testing for Known Open Source Vulnerabilities: Methodology

This ConsumerGram seeks to explore the degree to which Wi-Fi routers are potentially being left unpatched for known risks, making the routers themselves and the devices to which they are connected more susceptible to cybercrime and other online threats. Specifically, this analysis examines to what extent router manufacturers are providing secure products to consumers.

Failing to address known security flaws leaves consumer devices vulnerable to having their data compromised, leading to malicious activity, identity theft, fraud and espionage. The results presented here are based on a sample of 186 Wi-Fi routers from 14 different manufacturers that are or were available in the U.S. market and the firmware is currently available on the manufacturer's website (see the Appendix for the complete list of the routers included in the sample).

---

[2] Ibid.

[3] James Sanders, "Why router-based attacks could be the next big trend in cybersecurity," *TechRepublic*, April 17, 2018, https://www.techrepublic.com/article/why-router-based-attacks-could-be-the-next-big-trend-in-cybersecurity/.

[4] Robert Lemos, "Open-Source Could Mean an Open Door for Hackers," *Technology Review*, June 8, 2010, https://www.technologyreview.com/s/419257/open-source-could-mean-an-open-door-for-hackers/.

To test for the specific risks associated with the open source components used in the sampled routers, Insignary's Clarity program was used to scan embedded firmware for unpatched security vulnerabilities.[5]

Firmware: The Culprit for Security

Firmware is software that controls the basic functions of hardware devices, and it is at the heart of IoT and other connected devices. Even passwords are embedded in the firmware of IoT devices. As such, protecting firmware is the key to reducing cyber risks.

Fixing vulnerabilities lies partly in the hands of consumers who must do their homework and install firmware (software) updates. Although some hardware makers try to insulate users from update burdens by providing automatic updates, the average consumer has probably never considered taking the initiative to update their router's firmware. Because consumers rarely think about installing updates on their devices or are not even aware of potential security vulnerabilities, they tend not to consider firmware support.

In addition, manufacturers often do not provide user-friendly ways for consumers to update firmware or may even view building security protocols into their devices as an unnecessary expense. Sometimes accessing firmware updates requires consumers to have registered their products with the manufacturers, while other times these updates are not readily available online, and still other times somewhat older routers are not supported at all. This means that even consumers who try to update their router firmware might download outdated code that is all but useless against critical vulnerabilities discovered since its sale. Simply calling on consumers to turn their routers on and off is insufficient.

With the sharp rise in open source usage and the increasing number of vulnerabilities plaguing open source software, automated updates are by far the most feasible option to keep

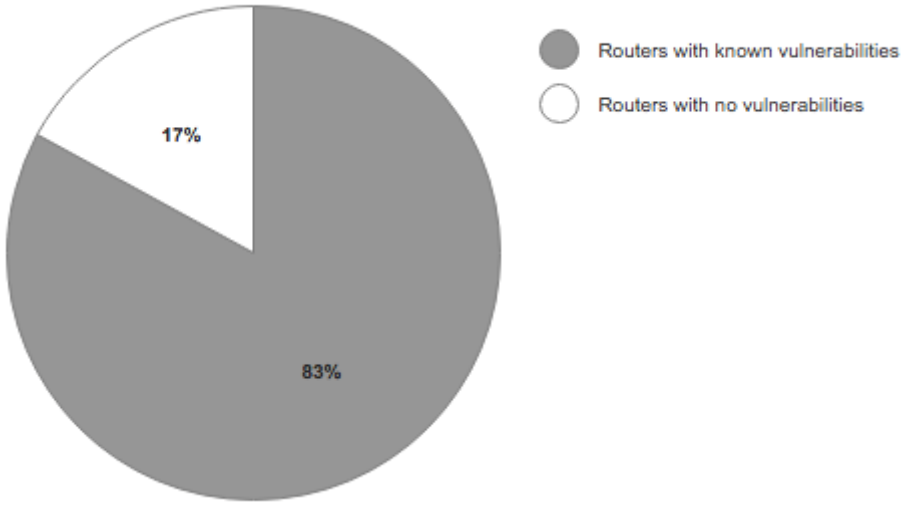
[5] The appropriate firmware was downloaded the week July 9, 2018, and the scans were performed the following week in order to minimize the probability of not testing the most updated firmware. For more information about Clarity, see www.insignary.com.

IoT devices and consumer data safe. However, in most cases, those automated updates do not appear to be happening. Unlike many consumers who may have outdated firmware on their older routers, this ConsumerGram scans the latest available manufacturer's firmware for known vulnerabilities.

Firmware Scans: The Results

Based on Insignary's Clarity scanning tool, our analysis shows that of the 186 sampled routers, 155 (83%) were found to have vulnerabilities to potential cyberattacks (see Figure 1) in the router firmware, with an average of 172 vulnerabilities per router, or 186 vulnerabilities per router for the identified 155 routers.[6] In total, there was a staggering number of 32,003 known vulnerabilities found in the sample.[7]

Figure 1: Percentage of Routers with Open Source and Known Vulnerabilities



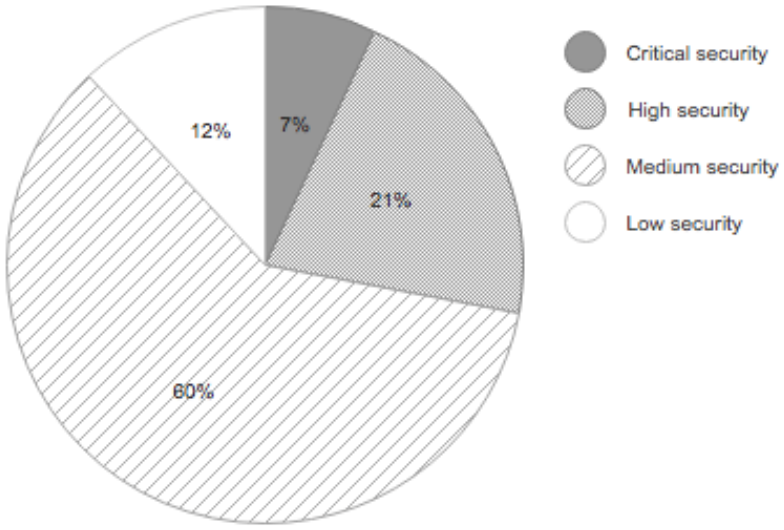
[6] We used MITRE Corporation's definition of vulnerabilities, "mistakes in open source software" that are recorded in a public database maintained by the MITRE Corporation (cve.mitre.org). Each vulnerability is identified with a unique CVE (Common Vulnerability and Exposure) identifier that contains information about a specific vulnerability's capacities and risks.

[7] Some routers were found to contain the same CVE under different components, suggesting that the potential risk is far higher than presented here.

The severity of each vulnerability is ranked by the National Vulnerability Database.[8] Based on the different scores, each vulnerability is ranked either "low," "medium," "high," or "critical" to reflect the severity of the potential risks associated with the vulnerability. High and critical vulnerabilities are more easily exploited, and it could cause more damage than low and medium vulnerabilities. High-risk vulnerabilities require very little knowledge or skill to exploit, but, unlike critical-risk vulnerabilities, they will not entirely compromise the system. The potential damage remains a concern, as exploited high-risk vulnerabilities can partially damage the system and cause information disclosure.

Within the sample, 28% of the vulnerabilities were considered high-risk and critical (see Figure 2). Our analysis shows that, on average, routers contained 12 critical vulnerabilities and 36 high-risk vulnerabilities, across the entire sample. The most common vulnerabilities were medium-risk, with an average of 103 vulnerabilities per router.

Figure 2: Distribution of Vulnerabilities Based on Security Risk Severity



[8] For further information, see the National Vulnerability Database website at https://nvd.nist.gov/vuln-metrics/cvss.

Wi-Fi Routers Security Exposures: Implications for IoT Devices

Internet-connected devices are now nearly ubiquitous in the United States and routers are a central point for connecting these IoT devices. These devices represent a growing constellation of tools, devices and appliances designed to collect, exchange and process information over the internet to provide access to an array of services and information.[9] They include security cameras, DVRs, printers, cars, baby monitors, data storage devices, refrigerators — even lightbulbs — and they have transformed how people, households and businesses interact with each other.

The security we want for our devices and software is rather simple. We want these electronic devices to be free from intrusion, and we want the data to be secure, not corruptible and certainly not distributable without the owner's authorization. Yet, our results show that these devices are highly vulnerable, and are becoming an increasingly attractive target for cyberattacks.

Symantec's annual Internet Security Threat Report found a 600% increase in IoT attacks in 2017. Routers were the most frequently exploited type of device, making up 33.6% of IoT attacks.[10] An IoT cyberattack can cause massive damage to the connected devices and harm to their owners. For instance, exploiting an Internet Protocol security camera gives an attacker not only access to the entire network the camera is connected to, it also gives them a direct video feed inside the property.[11]

[9] "Securing Your 'Internet of Things' Devices," U.S. Department of Justice (Computer Crime & Intellectual Property Section Criminal Division) and the Consumer Technology Association, July 2017, https://www.justice.gov/criminal-ccips/page/file/984001/download.
[10] "Internet Security Threat Report," Symantec, Volume 23, April 2018, https://www.symantec.com/security-center/threat-report.
[11] Lily Hay Newman, "An Elaborate Hack Shows How Much Damage IoT Bugs Can Do," *Wired*, April 16, 2018, https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/.

The 2017 Annual Cybercrime Report published by Cybersecurity Ventures predicts IoT devices to become the major technology crime driver in 2018, and that cybercrime damages will cost the world economy $6 trillion annually by 2021.[12]

Summary

The FBI's warning that Russian computer hackers had compromised hundreds of thousands of home and office routers highlighted the potential danger of open source routers, but the warning may have gone largely unnoticed by most consumers. In addition, as this ConsumerGram shows, Wi-Fi router manufacturers are neglecting to update their firmware for known vulnerabilities, and the problem is likely more pervasive for other IoT devices. When these security lapses occur, firmware can be fairly easily exploited by hackers with nefarious intentions.

The results of this study suggest that the most popular Wi-Fi routers in peoples' homes are inadequately updated for security, leaving IoT devices open to attacks with potentially disastrous results. Simply resetting your router is not enough. Keeping firmware patched for known online threats may be an expense for manufacturers, but not doing so leaves consumers to collectively bear the burden of potentially much higher costs from cybercrime.

Each of the 32,003 vulnerabilities identified in this report put consumers, our infrastructure, and our economy at risk. If this growing threat is to be countered effectively, manufacturers must commit more resources to identify and mitigate open source vulnerabilities on their devices and consumers must remain vigilant for potential threats that could compromise their personal data. With the IoT market expanding quickly for both residential and industrial applications, the need to secure firmware cannot be overstated.

[12] "2017 Cybercrime Report," Cybersecurity Ventures, October 16, 2017, https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

Appendix

List of routers included in the sample:

TP-Link

TL-WR94N V3
TL-WR94N V6
TL-WR845
TL-WR843
TL-WR843ND
TL-WR843ND
TL-WR841N
TL-WR840N
TL-WR802N
TL-WR743ND
TL-WR741ND
TL-WR740N
TL-WR710N
TL-WR702N
TL-WR1042ND
TL-WDR4300
TL-WDR3600
TL-WDR3500
ARCHER_C8
ARCHER_C7
ARCHER_C5
ARCHER_C50
ARCHER_C3200
ARCHER_C2
ARCHER_C20i
ARCHER_C20

ASUS

RT_N66R
RT_N600
RT_N16
RT_N56
RT_N12D1
RT_ACRH13
RT_AC5300
RT_AC3200
RT_AC1900
RT_AC3100
RT_AC1750
RT_AC1200G
RT_AC88U
RT_AC1200
RT_AC87U
RT_AC86U
RT_AC68U
RT_AC68P
RT_AC66U_B1
RT_AC66R
RT_AC66U
RT_AC56U
RT_AC56R
RT_AC55U
RT_AC51U
RT_GT_AC5300
RT_MAP_AC2200
BLUECAVE

AVM

FRITZBOX_6890
FRITZBOX_7590
FRITZBOX_7490

Belkin

F9K1124
F9K1119
F9K1123
F9K1116
F9K1118V2
F9K1115
F9K1102
F9K1113
F9K1105
F9K1103
F9K1009
F9K1010
F9K1002

Cerio

WP-300N
WMR-200N
IW-100
WM-200N
DT-300N_OS30
DT-100G-N
DT-300N
CW-400NAC_A2
CW-400NAC_A1

D-Link

DIR-878_REVA
DIR-882_REVA
DIR-867_REVA
DIR-859_REVA
DIR-842_REVERSIONB
DIR-842_REVERSIONC
COVR-3902
DIR-822-REVERSION2
DIR-605L_VERSIONB
DIR-605L_VERSIONA

HPE

VSR1000
MSR954

Linksys

WRT1900AC_V2
WRT3200ACM
WRT1900ACSV2
WRT1200ACV2
WRT54GL
WRT32X
EA9300
EA9500V2
EA9200
EA8300
EA8500
EA7500V2
EA7300
EA6900
EA6500V2
EA6400
EA6350V3
EA6300
EA6200
EA6100
EA5800
EA4500V3
EA3500
EA2750
EA2700
E8400
E2500
E1700
E1200
E900

NETGEAR

WNR3500L
WNR2200
WNR2500
WNR1000V3
WNR2000V3
WNDR4700
WNDR4500
WNDR3700
WNDR3400
R8900
R9000
R8300
R8500
R8000P
R8000
R7900P
R7900
R7800
R7300
R7500
R7000
R700P
R6900
R6700
R6900P
R6400
R6250
R6220
R6200
R6120
R6100
R6080
R6020
PR2000
N300
JR6150
AC1450
JNR3210

Sierra Wireless

MP70
RV50
LX60
GX450
ES450

TRENDnet

TEW-829DRU
TEW-812DRU
TEW-721BRM
TW-100
TEW-827DRU
TEW-818DRU
tew-817dtr
TEW-816DRM
TEW-731BR
TEW-714TRU
TEW-655BR3G

Ubiquiti Networks

UGW3
XG_8U_GWXG
PRO4_UGW4

Yamaha	Zyxel
RT810	NBG6815
FWX120	NBG6617
	NBG6515
	ARMOR_Z2_NBG6817
	NBG-418N
	ARMOR_Z1_NBG6816