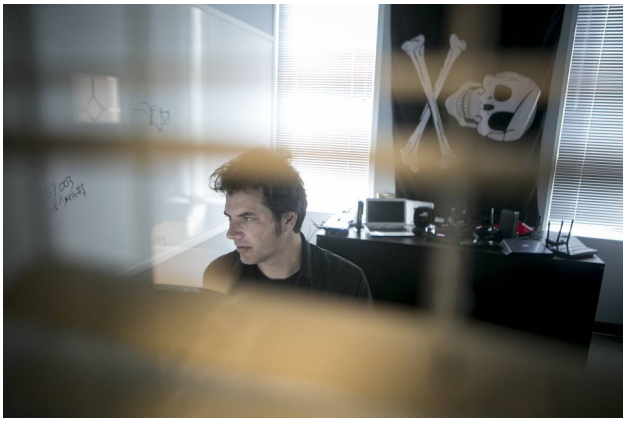
THE WALL STREET JOURNAL.

http://www.wsj.com/articles/rarely-patched-software-bugs-in-home-routers-cripple-security-1453136285

TECH

Rarely Patched Software Bugs in Home Routers Cripple Security

Wi-Fi devices, vulnerable to hackers, show difficulty of updating software after release



Tod Beardsley, a researcher at security company Rapid7, tested 20 new routers for The Wall Street Journal and found many had outdated software. *PHOTO: ILANA PANICH-LINSMAN FOR THE WALL STREET JOURNAL*

By **JENNIFER VALENTINO-DEVRIES**
Jan. 18, 2016 11:58 a.m. ET

In late 2014, a small Massachusetts software company got an ominous email: A computer-security researcher said a flaw in one of its programs put millions world-wide at risk of being hacked.

Engineers at the company, Allegro Software Development Corp., analyzed the flaw in the program, which can help users access the controls of home Internet routers. They quickly realized something strange: They had fixed this bug nearly 10 years earlier. But it lived on, even in new devices.

The reason: A component maker had included the 2002 version of Allegro's software with its chipset and hadn't updated it. Router makers used those chips in more than 10 million devices. The router makers said they didn't know a later version of Allegro's software fixed the bug.

The router flaw highlights an enduring problem in computer security: Fixing bugs once they have been released into the world is sometimes difficult and often overlooked. The flaw's creator must develop a fix, or "patch." Then it often must alert millions of technically unsophisticated users, who have to install the patch.

The chain can break at many points: Patches aren't distributed. Users aren't alerted or neglect to apply the patch. Hackers exploit any weak link.

In the case of the routers, Allegro said it couldn't apply the patch, because it doesn't have access to the devices. The company urges manufacturers to use the latest version of its software but can't require them to do so. "Nobody does that," said Loren Shade, vice president of marketing. "We've thought about it, but it's kind of hard to enforce."

To shed light on the problem, The Wall Street Journal commissioned a security researcher to test 20 popular Internet routers purchased new in the second half of 2015.

SEE THE TEST RESULTS

- Is Your Home Router Vulnerable to Hackers?

Ten arrived with known, documented security weaknesses. Tod Beardsley, a researcher at security company Rapid7 Inc. who conducted the tests, said the vulnerable routers had outdated "firmware," the programs that run a device. Four others had old firmware that had subsequent updates that Mr. Beardsley said could contain undocumented security problems.

Half of the group of 20 didn't let users easily check for new software during the standard setup process. Instead, users had to search on the Web or run optional programs. In addition, two routers incorrectly told users that updated software wasn't available, when in fact it was, and one directed users to download software that had a severe, documented security flaw.

The Journal's findings dovetail with those of Shahar Tal, a researcher formerly at Check Point Software Technologies Ltd. who helped find the Allegro bug, dubbed "Misfortune Cookie" because it allows hackers to attack the router using malicious Web cookies.

In scans over the Internet this spring, Mr. Tal found that 79% of the routers that initially contained Misfortune Cookie were still vulnerable, five months after the problem had been disclosed in public announcements and to the device makers.

Router makers are cutting corners by not checking the security of their products and failing to make efforts to keep customers informed of updates, he said. They "aren't paying the price for bad security," Mr. Tal said. "They're trying to cut prices by a dollar and win that contract from service provider X. Security isn't on their mind."

Router makers contacted by the Journal said security was important to them, and most said they had plans to improve how users are notified of new software—which often depends on a user noticing an update on the router's website. But several also said they fix routers according to how new they are; routers more than a couple of years old are less likely to get fixed.

Home routers are an easy target because manufacturers compete largely on price, for devices that typically sell for less than $100. Customers acquire the routers either from retailers or from Internet-service providers. Once routers are sold, manufacturers have little incentive to update them to improve security. Routers can remain in use for years after what manufacturers term their "end of life," meaning they no longer issue updates.

The same problem is evident in smartphones and the growing market for Internet-connected computers in everything from printers to television sets.

Security researchers recently showed how they could hijack an email account through a refrigerator by attacking the link it used to display the owner's Google calendar on the door's touch screen. Other researchers have demonstrated they can change the settings on Internet-connected medical devices, managed remotely by nurses and doctors, that infuse medicines into patients.

The Federal Trade Commission last year warned that companies entering these markets "may not have experience" with security. For users, the commission said, "It may be difficult or impossible to update the software or apply a patch."

Alphabet Inc.'s Google regularly updates its Android mobile-operating system, which runs roughly three-fourths of the world's smartphones, to patch security holes. But it generally relies on device makers and telecom carriers to distribute the new software. Device makers don't always distribute it, particularly for cheaper phones or those more than a year old.

University of Cambridge researchers in October said more than 85% of 20,000 Android devices they studied had at least one of 11 known critical vulnerabilities, largely because of "inaction by some manufacturers and network operators." That could allow a hacker to take control of a phone, usually through a malicious app.

"It's about economic incentives," said Alastair Beresford, a professor at Cambridge who studied the Android flaws. "Manufacturers are facing a choice in deploying limited resources. Do they deploy them on fixing bugs in products they have already sold years ago, or on producing the next handsets to sell?"

A Google spokeswoman said the company is working with manufacturers and carriers to distribute updates more quickly. Google also said it has made efforts to keep harmful apps, which hackers typically use to exploit a weakness in a device, off its Play Store. It said fewer than 1% of Android devices have installed a potentially harmful app.

Software on Apple Inc. devices is more commonly up-to-date, because Apple manufactures iPhones and iPads and controls more of the update process.

Automatic updates

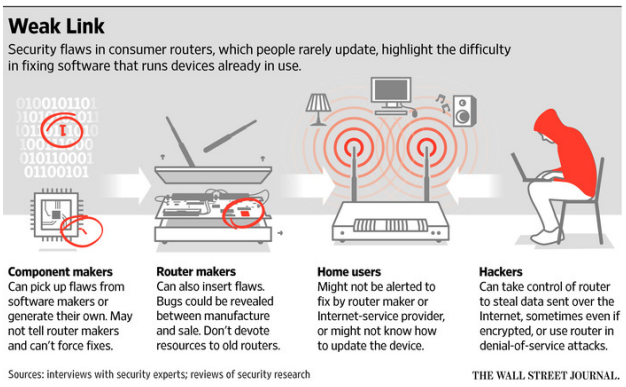
Software makers have wrestled with this issue—how to repair programs in widespread use—for decades. Software is written by humans, so it inevitably contains errors. Alan Paller, the founder and research director at the SANS Institute, a computer-security training center, said on average, 10,000 lines of code contain two to five errors. A program such as a Web browser has millions of lines of code, meaning it could have thousands of errors.

Following a series of breaches linked to Windows computers in the early 2000s, Microsoft Corp. started a unit to improve the security of its software. In late 2004, the company activated automatic updates by default on Windows machines. Some software, such as Google's Chrome Web browser, updates itself every few weeks.

Such efforts help more-secure software spread faster. Mozilla Corp. said more than 70% of users of its Firefox Web browser are on the latest version within 20 days of its release; since 2013, Firefox has updated on its own when the user restarts. Before that, when the browser prompted users to upgrade every few months, it took more than a year to get that many users on the newest software.

As security improves on personal computers, hackers seek other ways into networks. Routers make an inviting target.

Once in control of a router, hackers can access almost anything a user sends over the Internet, sometimes even if it is encrypted. In one incident reported in 2014, hackers hijacked routers to siphon off bank-account details from Polish consumers. Researchers in Spain last year tested 22 routers commonly used in Europe and found that each had at least one security vulnerability, including 60 flaws not previously seen.



Researchers at Internet-technology company Akamai Technologies Inc. said criminals also increasingly offer to infiltrate routers and use them to overwhelm targeted websites for a fee. Attack instigators may want to gain an advantage in online games, punish companies for bad service, camouflage another attack or extort money, said Eric Kobrin, Akamai's director of information security. Such router-type attacks were rare a year ago but in 2015 accounted for 10% to 20% of denial-of-service attacks, he said.

Mr. Kobrin said a group called Lizard Squad used routers and other home devices to direct malicious traffic that knocked gaming networks for Microsoft's Xbox and Sony Corp.'s PlayStation offline for hours on Christmas Day 2014.

None of the routers tested by the Journal was vulnerable to these types of attacks out of the box, with default settings in place. The Journal's tests found at least one flaw that has been used by hackers. "The Moon" worm was documented spreading among Linksys routers in 2014. A new Linksys E1200 N300 router purchased in July 2015 and tested by the Journal shipped with software from 2013 that still had the vulnerability the worm exploited.

Belkin International Inc., which owns the Linksys brand, initially said the 2013 software wasn't vulnerable to the bug, but after discussions with the Journal it acknowledged that users should update to newer software to protect from the hack. The company said all new routers are now shipping to stores with the later software.

No notification

Users can update device software to address such vulnerabilities, but most of the devices tested by the Journal didn't notify owners that new software was available. Two routers—one made by Belkin and one by Netgear Inc.—incorrectly told users there was no update.

In a statement, Netgear said new routers might arrive with old versions of firmware because it can take months for a router to get from a factory to a consumer. The router that incorrectly said an update wasn't available didn't work "as expected," Netgear said. Follow-up tests after the Journal contacted Netgear showed the router correctly indicated an update was available.

Belkin said its router couldn't find the update because the updated software hadn't been properly loaded on its computers. The company made the software available after being contacted by the Journal.

Another router, made by D-Link Systems Inc., directed U.S. users to download a version of the software that still contained a bug with the highest severity level in the National Institute of Standards and Technology's National Vulnerability Database. The bug, which allows a hacker to completely overtake a router, had been fixed by D-Link in May, but the patch was made available only on international D-Link sites and an obscure Internet forum.

After being contacted by the Journal, D-Link said in December that the company hadn't put the fixed firmware on its U.S. site because it had been conducting a "validation test" to confirm "that the firmware is succeeding." The update was put on the U.S. site in early January.

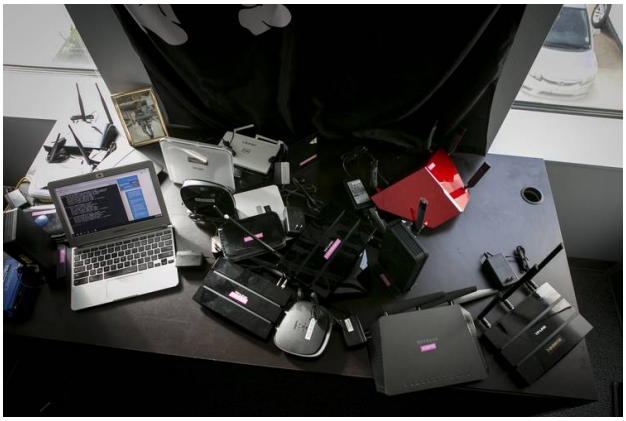
"I was surprised at the level of problems users would have just updating" the software, said Mr. Beardsley, the Rapid7 researcher who conducted the Journal's tests.

The tests found other security weaknesses. All but two of the 20 routers tested used insecure, widely known passwords by default and didn't require users to change them—a problem security researchers have cited for years. All 20 used network settings that security researchers say can be easily guessed by hackers. If combined with default login information, this can enable a hacker to seize control of the router.

The routers tested by Mr. Beardsley had fixed two problems regularly cited by security researchers in the past: None had remote administration settings enabled by default, and none was easily accessible over the Internet by openings that hackers regularly probe.

The Journal's tests didn't look for new vulnerabilities. Instead, they focused on known problems, to highlight weaknesses in the security chain. The Misfortune Cookie flaw was more prevalent in routers sold abroad than in the U.S., researchers said.

Mr. Tal, the researcher who found the bug, said he became interested in studying Allegro's software when he realized how widely it was used—and that the most-common version was from 2002. He and fellow researchers saw it on more than 200 models from dozens of router manufacturers but didn't understand why it was so prevalent.



Some of the routers tested by Rapid7 for the Journal. Software vulnerabilities can be exploited by hackers. *PHOTO: ILANA PANICH-LINSMAN FOR THE WALL STREET JOURNAL*

They eventually linked the software to MediaTek Inc., which had supplied chips for the vulnerable routers. MediaTek said the faulty software had been incorporated into the chip by a company it acquired and that maintenance fell through the cracks until 2014, when MediaTek learned about the Misfortune Cookie flaw.

"Once we were alerted, we acted quickly to minimize impact and remedy the issue for customers," by working with router makers to update the firmware, a MediaTek spokesman said.

Several router makers contacted by the Journal about Misfortune Cookie said they had issued updates on their websites that users could download to fix the bug.

Huawei Technologies Co., for example, published a fix for its two routers affected by Misfortune Cookie in December 2014, soon after being contacted by the researchers. In a statement, Huawei said it "expresses appreciation" to the researchers for disclosing the bug and urged people to download the latest firmware from the company's website.

TP-Link Technologies Co. initially had 23 affected models, according to the researchers. More than a year after the bug was publicized, the company's support site showed that three of the models had updates to address the vulnerability. TP-Link said seven additional models were scheduled to be updated before early February, but that other models were considered "end of life" and wouldn't be updated. The company is "prioritizing support for newer products, of which a larger portion are likely to still be in service," a company spokesman said.

But security pros say people often use these types of devices for a long time. Routers "are things you just set up and don't think about," said Mr. Tal, the researcher. "They stay out there for years and years until they break."

Is Your Home Router Vulnerable to Hackers?

Home routers used to connect to the Internet are plagued by security problems, a Wall Street Journal examination has found.

To test the extent of the problem, the Journal commissioned a computer-security researcher to evaluate 20 new popular wireless routers. The analysis focused on security issues, such as whether the device had up-to-date software or was vulnerable to known hacking exploits.

The Journal chose the routers from the top five manufacturers by U.S. sales, according to market research firm IDC. Specific models were chosen based on manufacturer reports and sales ranking on Amazon.com. All the routers were ordered new from Amazon in the second half of 2015 and tested with default settings in place.

Tod Beardsley, a researcher at security company Rapid7 Inc. who specializes in penetration testing and intrusion prevention and has evaluated routers and other devices in the past, tested the routers.

Mr. Beardsley examined:

- The router's "firmware," the programs that run the device, to see if it was the most current version; where the firmware wasn't current, the Journal noted whether subsequent versions specified that they fixed or improved security issues.
- The process for updating firmware, to see if it worked, and how easy it was.
- Whether the router used a common default login and password without forcing the user to change it.
- Whether the router was vulnerable to widely disseminated hacking techniques, using a

penetration-testing tool called Metasploit.

- Whether the router was easily accessible from the Internet.
- Whether remote administration is enabled by default, which is a security risk.
- Whether the router's network settings were easy for a hacker to guess.
- Whether the router encrypted communications when it was accessed remotely.

This is what the tests found. Favorable results are shown in green, problematic in red. Orange indicates weaknesses.

The companies' responses to the results are available by clicking on the "+" for each entry. Related Article » (http://www.wsj.com/articles/SB10629

Search:

Show 10 entries

Did Router	Would Misse Updat