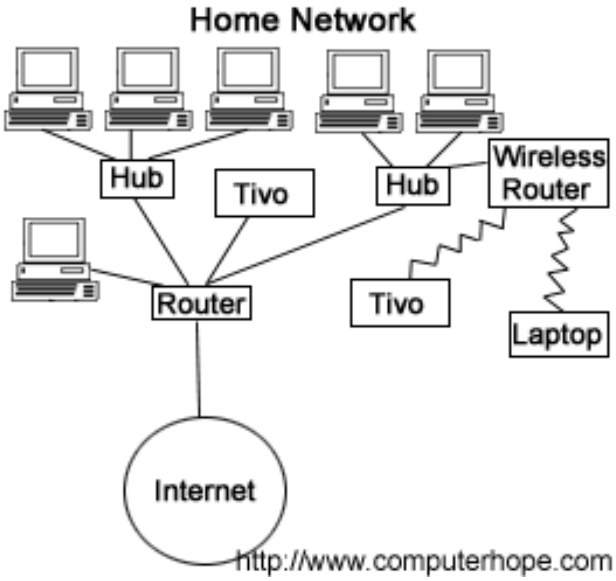
Macgill Davis
Ming Chow
Computer Security
December 12, 2014

SOHO Router Security

Abstract

Small Office / Home Office (SOHO) routers are used by nearly every single person with internet access in the United States. These routers typically support between 1 and 10 people and, as their name implies, are found primarily in homes and small businesses.[1] Despite the widespread use of SOHO routers, the computer security community has uncovered numerous vulnerabilities in nearly every popular SOHO router on the market. This paper will address the principal security vulnerabilities of SOHO routers and common attacking techniques for exploiting them. Subsequently, the paper will explore the best defenses to limit SOHO router hacking. Finally, this paper will explore the future of SOHO router defense as well as general implications of SOHO router vulnerabilities.



[1] Mitchell, Bradley. "What Is a SOHO Router." Web log post. *Http://compnetworking.about.com/*. About.com, n.d. Web.

Introduction

At its core a router is a networking device that connects computer networks by forwarding data packets. A few common functions of a router include taking incoming packets, analyzing packets, moving packets to another network, converting packets to another network interface, dropping packets, and directing packets to the appropriate locations. Routers are often used in home networks to share a single Internet connection with multiple computers.[2]

Most consumers use Small Office / Home Office (SOHO) routers to provide internet access in their homes, connecting their computer to the Internet through the router. Thus all data exchanged between a home computer and the Internet almost always passes through a SOHO router including all photo uploads to Facebook, bank account logins and Google searches. Acting as middlemen with access to a wealth of information, SOHO routers compose a vital link in the chain of internet connectivity.

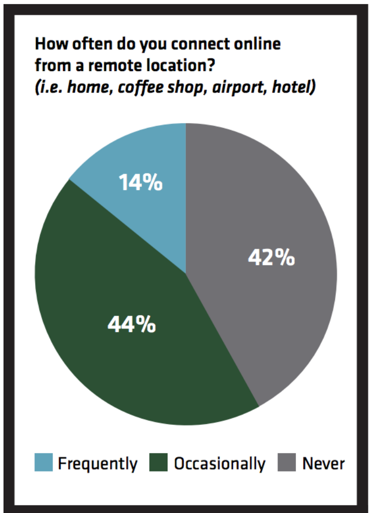


FIG. 1 *How often do you connect online from a remote location?*

Furthermore, SOHO routers are the most common way the average American internet user connects to the Internet. According to the latest census, roughly 318 million people currently live in the United States.[3] According to the United States' Census Bureau, 74.4 percent of the population, or 237 million Americans, have household

[2] "What Is a Router?" *Computer Hope*. N.p., n.d. Web. <http://www.computerhope.com/jargon/r/router.htm>.

[3] CIA. "The World Factbook." *CIA Factbook*. N.p., July 2014. Web. 11 Dec. 2014. <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html>.

access to the internet.[4] Most of those connections are enabled through SOHO routers. While worldwide internet access is more varied, the number of internet users is projected to pass three billion in the coming year and many of those users rely on SOHO routers.[5]

SOHO routers increasingly handle business data in addition to personal data. Many employees often work from home, bringing their data out in the open from behind corporate firewalls.[6] Additionally, many businesses are beginning to use SOHO routers in the office. The current trends indicate that the use and significance of SOHO routers and the Internet will continue to grow in lockstep.

Current State of Affairs

In spite of the importance and extensive utilization of SOHO routers, numerous vulnerabilities have been exposed that put the security of *most* American's at risk of attack. Sadly, common and well-documented attack techniques compose most of the known vulnerabilities. In fact, SOHO router security has many of the same characteristics found in other spheres of computer security with both manufacturers and users at fault. On the development front, vendors continue to overlook or discount security in production and consequently deliver SOHO routers susceptible to attack.

[4] Bureau, U.s. Census. *Computer and Internet Use in the United States: 2013* (n.d.). *Census.gov*. United States Government, Nov. 2014. Web. 10 Dec. 2014. <http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf>.

[5]"Number of Internet Users." *Internet Live Stats*. N.p., n.d. Web. 10 Dec. 2014. <http://www.internetlivestats.com/internet-users/>.

[6] Tripwire. "SOHO Wireless Router (In)Security." *Tripwire.com*. N.p., Nov. 2014. Web. 9 Dec. 2014. <http://www.tripwire.com/register/soho-wireless-router-insecurity/showMeta/2/>.

On the opposite side of the counter, the average user is often unaware of these security vulnerabilities or the necessary precautions to take to strengthen defenses. These circumstances result in SOHO routers ripe for attacks that can have extensive and serious implications. Once a router has been compromised everything once protected by its firewall becomes vulnerable and an attacker can monitor, redirect, block or tamper with data the router receives.

Awareness

In recent years coverage of SOHO router security has grown substantially. In February 2014, the Vulnerability and Exposure Research Team (VERT) at the software security company Tripwire released “SOHO Router (In)Security”, a report regarding the status of SOHO router security. VERT found that 80 percent of Amazon’s best-selling SOHO wireless routers have security vulnerabilities and 34 percent have publicly documented exploits that make it relatively simple for attackers” to undertake attacks.[7]

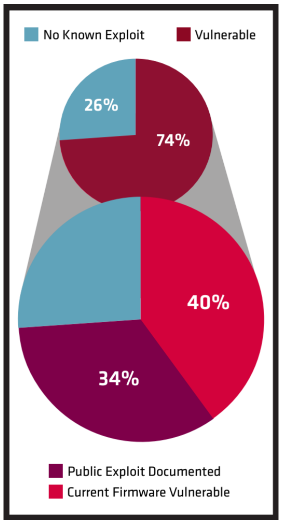


FIG. 2 *Amazon Top 50 Wireless Router Vulnerability Breakdown*

In April 2013, researchers at Independent Security Evaluators (ISE) published a case study on SOHO router security. From their selection of 13 of the most common SOHO routers, ISE researchers discovered that all 13 could be taken over from the

[7] “SOHO Router (In)Security”, Tripwire

local area network (LAN) and 11 of 13 could be taken over from the wider area network (WAN).[8] Table I in the Appendix summarizes the case study.

At the most recent DEF CON, one of the largest annual computer security conferences in the world, ISE followed up their case study by sponsoring a SOHO router hacking contested aptly titled “SOHOpelessly Broken” in the hopes of increasing awareness for SOHO router security.[9] Stephen Bono, co-founder of ISE, said that ISE “decided to open it up to the hacker community at large, have a contest, and shine a big spotlight on the issue, and down the road, maybe manufacturers will take security more seriously.”[10] Teams and individuals worked to successfully compromise a range of the most common SOHO routers found on the market. The results of the contest revealed persistent broad deficiencies in today’s SOHO router security, as several new flaws were unearthed and many known flaws remained un-patched.[11]

Vulnerabilities

Each SOHO router manufactured by a different vendor will have its own specific vulnerabilities and processes to exploit those vulnerabilities but many common flaws were found within routers produced by unrelated vendors. Below a few of the some of the most vulnerabilities across all SOHO routers are detailed including Cross-Site

[8] Holcombe, Jacob. "SOHO Routers Case Study." *Independent Security Evaluators*. N.p., 2013. Web. 8 Dec. 2014. <http://www.securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php>.

[9] https://www.sohopelesslybroken.com/

[10] Mimoso, Michael. "DEF CON HOSTING SOHO WIRELESS ROUTER HACKING CONTEST." *Threatpost*. N.p., 28 July 2014. Web. 10 Dec. 2014. <http://threatpost.com/def-con-hosting-soho-wireless-router-hacking-contest/107463>.

[11] Independent Security Evaluators. "DEF CON 22 SOHOpelessly Broken Results." *SOHOpelessly Broken*. N.p., Aug. 2014. Web. 12 Dec. 2014. <https://www.sohopelesslybroken.com/contests/defcon22/results.php>.

Scripting (XSS), Cross-Site Request Forgery (CSRF), Buffer Overflow, Authentication Bypass as well as data encryption flaws.

Web Attacks

Nearly every SOHO router on the market provides a web interface for users to more easily configure they network. While this undoubtedly eases use, it opens up another portal that attackers can exploit using techniques that are common across the Internet such as *Cross-Site Request Forgery*, *Code Injection*, and *Directory Traversal*.

Cross-Site Request Forgery (CSFR) occurs when an attacker forces a user to execute commands unknowingly when a web application in which the user is already authenticated. Often times CSFR requests involve a bit of social engineering to trick the user into clicking that allows for the CSRF and commands to be executed. Nearly every router that ISE examined contained CSRF vulnerabilities that allowed an attacker to change the password or username of the server, add another admin account or allow remote control access.

Code Injection revolves around the server failing to sanitize or validate input from the user. The lack of validation (or perhaps granting of trust as an attacker would like to think of it) allows an attacker to input code that will be executed on the server side. *Command Injection* includes *Cross-Site Scripting* (XSS) where the attacker inputs script into a webpage, *Database Injection* when the attacker inputs valid database queries to extract data, or *Command Injection* when the attacker inputs commands to the host operating system. Username and password fields are vulnerable to these forms of attacks if the client-side input is not validated. Many vendors failed to validate any input and therefore left their server open to attack by even a amateur attacker. ISE notes an example with the TRENDnet TEW-812DRU router that failed to validate input and allowed the injection of “operating system commands into the vulnerable web application, which ultimately lead to its compromise.”[12]

Directory Traversal is another classic web attack that often arises from insufficient validation of input and allows the attacker to access files outside of the current folder. The attacker is free to traverse across the website and extract sensitive information. A classic example of directory traversal is “../../../../../../../../../etc/passwd” in which the attacker uses the ‘../‘ to climb into the root directory and then access the password folder from there. Researchers found the DLINK DIR-865L router particularly susceptible to a directory traversal attack.[13]

Added Functionality

One major cause of SOHO router vulnerabilities arises from extensive amount of additional services modern routers provide including SMB, NetBios, HTTP(S), FTP, UPnP, Telnet and more. Additional functionality is not inherently bad for users and, on the contrary, is often a benefit. However from a security standpoint, the addition of more services signifies more attack vectors through which an attacker can gain access. On a group of routers with USB storage attached, ISE found that on average a router had twenty-two ports open.[14]

Furthermore, vendors have shown little desire or ability to erect the proper security defenses around these added services. Several network service software

[12] "SOHO Routers Case Study”, Jacob Holcombe

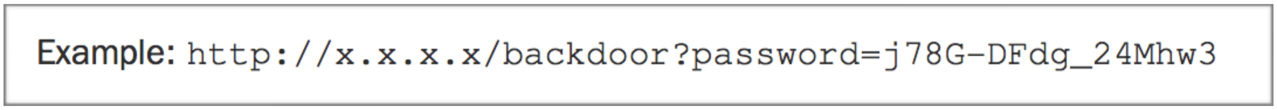
[13] Holcombe, Jacob. *SOHO Network Equipment*. Rep. Baltimore: Independent Security Evaluators, 2014. < https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf>

[14] “SOHO Network Equipment, Jacob Holcombe

packages fail to perform bound checking and are susceptible to *Buffer Overflow*. This failure allows an attacker to overflow the buffer, overwrite memory and corrupt the host system. In the *SOHO Router Vulnerability Database* compiled by ISE, the Broadcom ACSD network service that scans and selects low interference Wi-Fi channels was shown to permit buffer overflow that “could lead to total compromise of the entire router.”[15]

Backdoors

In software, *Backdoors* are ways to bypass authentication. Many times they are employed in development so that developers can easily access and edit processes that would normally require authentication. There almost never exists a valid reason that *backdoors* exist in production. Nonetheless, ISE researchers found the *same* backdoor in several routers manufactured by *different* vendors. In TRENDnet and Linksys routers the URL allows for authentication bypass. ISE believes that the *backdoor* “is an artifact of using sample code, or example code provided by a chipset manufacture, where the authors (maybe carelessly) chose to copy it.”[16] This negligence by multiple of the biggest router vendors reveals a greater lack of security consideration widespread in the manufacture of SOHO routers.



Example: `http://x.x.x.x/backdoor?password=j78G-DFdg_24Mhw3`

[15] Independent Security Evaluators. "SOHO Router Vulnerability Catalogue." (n.d.): n. pag. *Independent Security Evaluators*. Summer 2014. Web. 8 Dec. 2014. <https://securityevaluators.com/knowledge/case_studies/routers/Vulnerability_Catalog.pdf>.

[16] “SOHO Network Equipment, Jacob Holcombe

Security Mindset

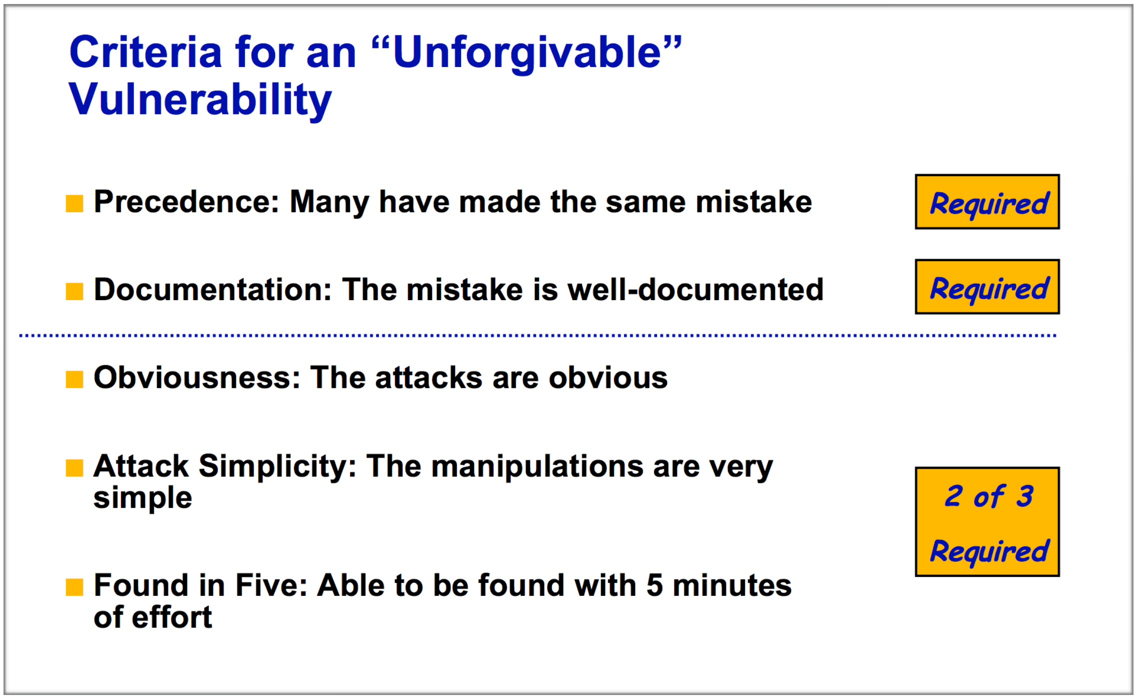
The lack of security mindset among SOHO router vendors appears in the plethora of simple vulnerabilities and lack of precaution. These include authentication bypass, absence of any data encryption, clear text storage of sensitive data, improper file and service permissions, unauthenticated read/write access to memory and the assumption of security on the (W)LAN. Clear text storage of password files on some routers allow attackers to download passwords in plaintext. Similarly, username and passwords were rarely encrypted on the router web interfaces. This assumes a level of security present on the LAN that is rarely assured. To compound this issue, even when security precautions are available they are rarely by enabled by default. Of the routers that ISE examined only 40 percent had HTTPS capability and only 20 percent had HTTPS running by default.[17]

Any security expert would not categorize most of the mentioned vulnerabilities as particularly novel, creative or unique to SOHO routers. On the contrary, the vulnerabilities covered include some of the most common attacks whose existence has been known for years. Frustratingly, nearly all of these flaws have simple, effective and easy-to-implement defenses that prevent their successful execution. Computer security expert and one of the creators of the *Common Vulnerabilities and Exposures* (CVE)[18], Steve Christey assembled a list of “Unforgivable Security Vulnerabilities” that must meet the requirements of precedence, documentation, obviousness, attack simplicity and

[17] “SOHO Network Equipment, Jacob Holcombe

[18] The Common Vulnerabilities and Exposures is a dictionary of publicly known security vulnerabilities and exposures that serves as the basis for most modern security documentation.

found in five.[19] *Directory Traversal, Buffer Overflow, Remote File Inclusion, XSS, SQL injection, World-Writable Files,* and *Authentication Bypass* compose seven of the thirteen of the “Unforgivable Security Vulnerabilities”. Furthermore, many of those vulnerabilities are listed in the Common Weakness Enumeration (CWE) “Top 25 Most Dangerous Software Errors”, including several that are in the top ten of the list.[20] The fact that router vendors have failed to construct proper defenses for such basic security flaws has left many of the internet connections across the country open to attack.



Criteria for an “Unforgivable” Vulnerability

- **Precedence: Many have made the same mistake** — ***Required***
- **Documentation: The mistake is well-documented** — ***Required***

- **Obviousness: The attacks are obvious**
- **Attack Simplicity: The manipulations are very simple**
- **Found in Five: Able to be found with 5 minutes of effort**

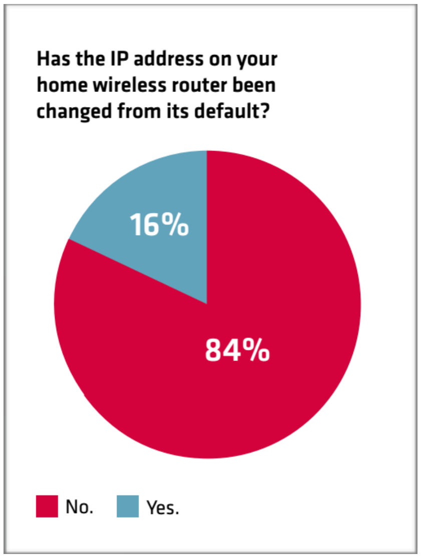
2 of 3 Required

[19] Christey, Steve. "Unforgivable Vulnerabilities." (n.d.): n. pag. *MITRE*. 7 Aug. 2007. Web. 5 Dec. 2014. <https://cve.mitre.org/docs/docs-2007/unforgivablevulns_bh.pdf>.

[20] http://cwe.mitre.org/top25/

The User

The same security issues relating to end-users that plague all of computer security appear in SOHO router security. A major challenge with SOHO router security is that it makes the average internet user the administrator of the entire network. Rather than a professional IT worker, the average user with limited technical skills and understanding becomes responsible for setting router defaults, updating firmware and setting authentication credentials. Users rarely change username, password or the IP address of their router allowing anyone on their LAN to navigate to the router's web login interface and brute force their way into the system. This generally does not take much time as most default username and passwords are some combination of 'admin' and 'password', the first guesses of any attacker or brute-force software. Additionally, when security vulnerabilities are found in routers or firmware, users rarely patch or update their router software. In fact, users rarely even think about their router unless the internet stops working. This allows attackers to gain entry and gather information with little worry of being identified.



After Compromise

After an attacker compromises a router he or she has several alternatives to gather information on the network and the router users. An attacker can undertake a *Man-In-The-Middle* (MITM) attack in which the users believe they are communicating privately but in reality all the data is being passed through the attacker. The attacker can forward the user to the webpages of his or her liking. The attacker can also silently gather information on all sites the users are visiting and grab unencrypted data like photos, passwords or credit card numbers. They can alter HTTP and DNS requests so that the users download malware without any idea that they are being attacked. Attackers could also place a *Trojan Horse* in the network that could disable routers at any given moment and create a Denial of Service attack.[21] In recent years the number and scope of router attacks have increased substantially. Router hacking in Brazil through one firmware vulnerability compromised 4.5 million routers and affected millions of internet users in 2011.[22] In March 2014, 300,000 infected routers led to a *Denial of Service* attack on millions in Europe and Asia.[23]

Trojan Horse and *MITM* attacks compose only a couple examples of potential routes of action available to attackers after a router has been compromised and many other options exist.

Why now?

Despite the recent surge in security vulnerabilities discovered, Christey does not believe any specific phenomenon related to SOHO routers has occurred but rather views the process as a common cycle in the security industry. Security vulnerabilities exist in products and software for years without anyone noticing. Eventually, researchers or attackers identify a class of products with security deficiencies and

[21] “SOHO Router (In)Security”, Tripwire

[22] Assolini, Fabio. "The Tale of One Thousand and One DSL Modems." *Securelist Information about Viruses Hackers and Spam*. N.p., 01 Oct. 2012. Web. 12 Dec. 2014. <http://securelist.com/blog/research/57776/the-tale-of-one-thousand-and-one-dsl-modems/>.

[23] Mimoso, Michael. "300,000 Compromised Routers Redirecting Traffic to Attacker Sites." *Threatpost*. N.p., 03 Mar. 2014. Web. 12 Dec. 2014. <http://threatpost.com/300000-compromised-routers-redirecting-traffic-to-attacker-sites/104589>.

suddenly a flood of vulnerabilities are discovered and awareness is raised. Christey refers to this as the *Pig Pile Effect* and he believes that the SOHO router industry is currently undergoing this process.[24] Thus, the security vulnerabilities in SOHO routers have most likely existed for years without anyone noticing. “It is not worse. It has always been bad. It is just that people didn’t look before” says Christey in reference to the *Pig Pile Effect.* Fortunately for SOHO router users, the *Pig Pile Effect* usually results in the most obvious and simple vulnerabilities being patched. Although vulnerabilities will always exist, Christey states “the general pattern is that researchers and vendors will get rid of the low hanging fruit first.”[25]

The Nature of the Market

Although many of the security vulnerabilities are inexcusable, part of the difficulty in securing SOHO routers derives from the nature of the router market. The router market is extremely competitive and vendors are constantly rushing to get products to market. Vendors and consumers tend to value functionality and speed and rarely consider security. Vendors rely on middleware and third-party software for functionality and rarely test how those programs fit into their system from a security perspective. Routers tend to have long lifespans and vendors rarely have the financial incentive to patch older models even if they are still in widespread use. When vendors do patch models, they tend to only patch the models explicitly shown to have vulnerabilities and not their sister products that often have the same software and therefore the same

[24] Steve Christey Phone Interview, December 5, 2014

[25] Steve Christey Phone Interview, December 5, 2014

vulnerabilities.[26] All these combine to make SOHO routers extremely vulnerable product group.

Christey also believes problems arise from the fact that most programmers do not know how to program for security. Programming for security involves thinking like an attacker and preparing for bad input. A SOHO route might have a login page to perform authentication. Under normal usage, the assumption would be that the user always goes through that login page for authentication. But if an attacker knows of another page that does not require authentication he could potentially bypass the login page and gain access to the entire application. "Vulnerabilities and attacks that exploit those vulnerabilities are not well behaved" says Christey.[27] Programmers need to learn to program for security and very few college programs or technical schools stress security.

SOHO Router Defense

Many of the current known vulnerabilities of routers arise from a failure to validate user input. As Tufts University computer security Professor Ming Chow coined, the top three rules of computer security are: "never trust user input, never trust user input and never trust user input."[28] Validation of user input solves many problems like XSS, *Buffer Overflow*, and *Command Injection*. A security analysis of routers would quickly reveal most issues before production. A simple static analysis of code would

[26] "SOHO Router (In)Security", Tripwire

[27] Steve Christey Phone Interview, December 5, 2014

[28] Ming Chow Class Lecture 15, Fall 2014

show the backdoors and authentication bypass due to code while a dynamic analysis can test for bizarre inputs. Flaws like CSFR can be fixed by adding a random session authentication token, something that many sites across the internet do to protect against attacks.The vendors must place a higher value on security if they want to ensure the protection of users data. Users can help incentivize in routers by placing a higher value on better defended models when purchasing new routers.

Although many of the security flaws must be fixed by vendors, there are several precautions users can take to limit their routers vulnerability. Remote management should almost never be enabled as it allows attackers to enter the admin mode without connecting to the LAN. Users should change the default settings on their routers immediately. That includes changing the admin's password and changing the ip address of the router from the default setting which can easily be done in most web interfaces.

If encryption is provided by the router it should be turned on at all times. Finally, it is important that users keep the firmware on the router updated and make sure the firewall is turned on.

Conclusion

It is clear that SOHO routers require immense improvement in their security. Vendors need to work on fixing the blatant flaws that currently exist and users need be more aware of the precautions to take in regards to router security. Fortunately the computer security has identified this issue and is raising awareness. Hopefully within the next few years most of these vulnerabilities will be patched. However, vulnerabilities will always exist and therefore security should never stray from the minds of users or vendors.

Bibliography

1. Mitchell, Bradley. "What Is a SOHO Router." Web log post. *Http://compnetworking.about.com/*. About.com, n.d. Web.

2. "What Is a Router?" *Computer Hope*. N.p., n.d. Web. <http://www.computerhope.com/jargon/r/router.htm>.

3. CIA. "The World Factbook." *CIA Factbook*. N.p., July 2014. Web. 11 Dec. 2014. <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html>.

4. Bureau, U.s. Census. *Computer and Internet Use in the United States: 2013* (n.d.): n. pag. *Census.gov*. United States Government, Nov. 2014. Web. 10 Dec. 2014. <http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf>.

5. "Number of Internet Users." *Internet Live Stats*. N.p., n.d. Web. 10 Dec. 2014. <http://www.internetlivestats.com/internet-users/>.

6. Tripwire. "SOHO Wireless Router (In)Security." *Tripwire.com*. N.p., Nov. 2014. Web. 9 Dec. 2014. <http://www.tripwire.com/register/soho-wireless-router-insecurity/showMeta/2/>.

7. https://www.sohopelesslybroken.com/

8. Mimoso, Michael. "DEF CON HOSTING SOHO WIRELESS ROUTER HACKING CONTEST." *Threatpost*. N.p., 28 July 2014. Web. 10 Dec. 2014. <http://threatpost.com/def-con-hosting-soho-wireless-router-hacking-contest/107463>.

9. Holcombe, Jacob. "SOHO Routers Case Study." *Independent Security Evaluators*. N.p., 2013. Web. 8 Dec. 2014. <http://www.securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php>.

10. Independent Security Evaluators. "DEF CON 22 SOHOpelessly Broken Results." *SOHOpelessly Broken*. N.p., Aug. 2014. Web. 12 Dec. 2014. <https://www.sohopelesslybroken.com/contests/defcon22/results.php>.

11. Holcombe, Jacob. *SOHO Network Equipment*. Rep. Baltimore: Independent Security Evaluators, 2014. < https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf>

12. Independent Security Evaluators. "SOHO Router Vulnerability Catalogue." (n.d.): n. pag. *Independent Security Evaluators*. Summer 2014. Web. 8 Dec. 2014. <https://securityevaluators.com/knowledge/case_studies/routers/Vulnerability_Catalog.pdf>.

13. Assolini, Fabio. "The Tale of One Thousand and One DSL Modems." *Securelist Information about Viruses Hackers and Spam*. N.p., 01 Oct. 2012. Web. 12 Dec. 2014. <http://securelist.com/blog/research/57776/the-tale-of-one-thousand-and-one-dsl-modems/>.

14. Mimoso, Michael. "300,000 Compromised Routers Redirecting Traffic to Attacker Sites." *Threatpost*. N.p., 03 Mar. 2014. Web. 12 Dec. 2014. <http://threatpost.com/300000-compromised-routers-redirecting-traffic-to-attacker-sites/104589>.

15. Christey, Steve. "Unforgivable Vulnerabilities." (n.d.). *MITRE*. 7 Aug. 2007. Web. 5 Dec. 2014. <https://cve.mitre.org/docs/docs-2007/unforgivablevulns_bh.pdf>.

16. Steve Christey Phone Interview, December 5, 2014.

Appendix

	Remote Adversary			Local Adversary		
Router	Trivial	Unauthenticated	Authenticated	Trivial	Unauthenticated	Authenticated
Linksys WRT310Nv2			X			X
Belkin F5D8236-4 v2			X			X
Belkin N300		X	X	X	X	X
Belkin N900		X	X	X	X	X
Netgear WNDR4700				X	X	X
TP-Link WR1043N			X			X
Verizon Actiontec			X			X
D-Link DIR-865L			X			X
ASUS RT-N56U			X			X
ASUS RT-AC66U			X			X
Linksys EA6500						X
Netgear WNR3500			X	X	X	X
TRENDnet TEW-812DRU			X			X

Has the administrative password to your home wireless router been changed from its default?