Global Information Assurance Certification Paper

Router backdoors - Can you trust your vendor?

GIAC (GSEC) Gold Certification

Author: Christoph Eckstein, christopheckstein.sec@gmx.net
Advisor: Rob VandenBrink

Accepted: September 27th 2014

Abstract

With the discovery of admin backdoors in network devices of Barracuda in January last year, it once again has become apparent that internet-facing network devices are vulnerable to unauthorized remote access. It was found that 80% of best-selling routers have security vulnerabilities that may be exploited to gain unauthorized remote access. With increasing reports of router vulnerabilities found like the ones in Cisco NX based devices in early 2014, the question arises whether these routers and network devices are doing a good job in keeping their users' networks and personal data secure. Even worse, with hidden built-in vendor backdoors and default logins found in network devices, the question arises if users can trust their vendors to uphold security as a key feature of their products. Apart from analyzing vulnerability disclosures in the past, this paper outlines techniques und provides suggestions to mitigate the risk associated with router vulnerabilities.

1. Introduction

With the discovery of admin (root level) backdoors in network devices of Barracuda in January last year, it once again has become apparent that internet-facing network devices are vulnerable to unauthorized remote access (Goodin, Secret backdoors found in firewall, VPN gear from Barracuda Networks, 2013). It was found that 80% of best-selling routers have security vulnerabilities that may be exploited to gain unauthorized remote access (Gilbert, 2014). With increasing reports of router vulnerabilities found like the ones in Cisco NX based devices in early 2014 (Cisco Systems, Inc., 2014), the question arises whether these routers and network devices are doing a good job in keeping their users' networks and personal data secure. Even worse, with hidden built-in vendor backdoors (Kirk, 2013) and default logins found in network devices (Cisco Systems, Inc., 2006), the question arises if users can trust their vendors to uphold security as a key feature of their products. And moreover, it raises the question if routers will provide the security users expect to protect their personal networks and data.

Network devices like routers are key parts of network infrastructures. They are supposed to separate the internet from the trusted internal or private network. They are supposed to keep private networks secure. Even more important, they are supposed to protect our personal data and prevent unauthorized access. Network storage devices become more and more popular in private homes and modern routers are capable of providing network access to USB storage devices connected to them. Subsequently, vulnerabilities and backdoors that allow unauthorized remote access represent a serious threat to the privacy of personal data stored on such devices (Independent Security Evaluators, 2013). Furthermore, with root level access malicious attackers are able to manipulate and reroute traffic. A DNS manipulation might allow an attacker to reroute online banking traffic to his own malicious server and thereby intercept the users' personal banking information.

This problem is even more pressing for SOHO devices (small office and home office), which are often installed as the only security perimeter defense. Unlike larger organization private homes and smaller organization might tend to rely on a simpler network infrastructure due to feasibility and budgetary reasons. Even with multiple

security layers, users' personal information is not necessarily safe. For example, if all layers rely on hardware from the same vendor, all of them might be susceptible to the same vulnerability (Craig, 2013).

With the threat of unauthorized access to our personal data presented through router backdoors and with increasing reports of the discovery of such backdoors, it may be reasonable to ask whether users can trust their router or vendor to protect their personal data; and consequently, what vendors and users could do to make sure their router and personal data are secure. This paper will firstly examine past experiences with backdoors in routers. Secondly, it will outline what users and vendors could do to prevent and eliminate backdoors and security risks associated with backdoors.

2. Backdoor definition

In the context of this paper "backdoor" generally describes the ability to remotely gain unauthorized access to routers or connected systems and data over the internet through some kind of security vulnerability or vulnerable configuration. Vulnerabilities include information disclosure or configuration manipulation through improper input validation (DefenseCode Security Advisory, 2013), hidden built-in backdoors (Craig, 2013), default configurations and passwords (Cisco Systems, Inc., 2006) and authentication bypass through a web service (Lovett, ASUS RT-N66U Router - HTTPS Directory traversal and full file access and credential disclosure vuln, 2013). Most backdoors manifest through unintentional implementation errors like improper input validation or inadequate security testing by the vendor. But reports also disclose purposely built-in backdoors by vendors (Kirk, 2013).

Furthermore, there are vulnerabilities and additional ways to compromise a router through CSRF (cross-site-request-forgery) or vulnerabilities in wireless LAN deployment (Independent Security Evaluators, 2013). In case of wireless LAN, a malicious attacker needs physical proximity to the target. In case of CSRF vulnerability in the administration web interface, an attacker will have to stage his attack through a victim within the private network. Although there are many different types of backdoors, this

paper concentrates on backdoors that manifest through direct remote access to the router itself over the internet.

3. Router backdoor example

In the following the authentication bypass vulnerability discovered in ASUS RT-N66U routers in June 2013 is demonstrated as an example of a backdoor (Lovett, ASUS RT-N66U Router - HTTPS Directory traversal and full file access and credential disclosure vuln, 2013). Several other ASUS routers were affected by this vulnerability as well. The vulnerability itself was found in connection with the ASUS "AiCloud" services. ASUS offers the AiCloud services for a range of their router products, including the RT-N66U. According to the ASUS homepage, AiCloud "… links your home network and online Web storage service together and lets you access it through the AiCloud mobile app on your iOS or Android smartphone or through a personalized URL in a Web browser" (ASUSTeK Computer Inc., 2014). AiCloud includes three different services, which can be activated independently. "Cloud Disk" basically makes connected USB devices accessible through the WAN interface via a web interface. "Smart Access" enables remote configuration options like "Wake-on-LAN", which allows starting computers in the local area network without physical interaction. "Smart Sync" offers automated synchronization capabilities between the ASUS cloud storage, the router and even other AiCloud enabled devices. The vulnerability demonstrated in the following is present when any one of these AiCloud services is activated on the router.

The example will illustrate how easily personal data can be exposed to the internet by vulnerabilities in the router's implementation of services. In this case, the web service offered with AiCloud to access personal data stored on USB devices connected to the router.

3.1. Test configuration

The test configuration setup contains three systems as shown in Figure 1 - Network diagram of test configuration. The first system is a router with a DHCP server. This router simulates the internet and is therefore called "internet router". The second system, the ASUS RT-N66U router itself, is connected to the "internet router" via its

WAN (wide area network) interface, which would normally connect the router to the internet. Although a local IP is automatically assigned to the WAN interface of the ASUS router, in this case it simulates a connection to the internet. The WAN interface functions the same way as if the ISP (internet service provider) would have assigned a public IP to the router's WAN interface. The local network side of the ASUS router is of no interest for this test configuration, the test focus on the WAN interface. The third system is the test system, in this case a computer running the SamuraiWTF distribution. The test system is assigned an IP address within the same network or subnet as the ASUS router's WAN interface. This test configuration allows running tests from the test system against the ASUS router's WAN interface as if they were done over the internet.

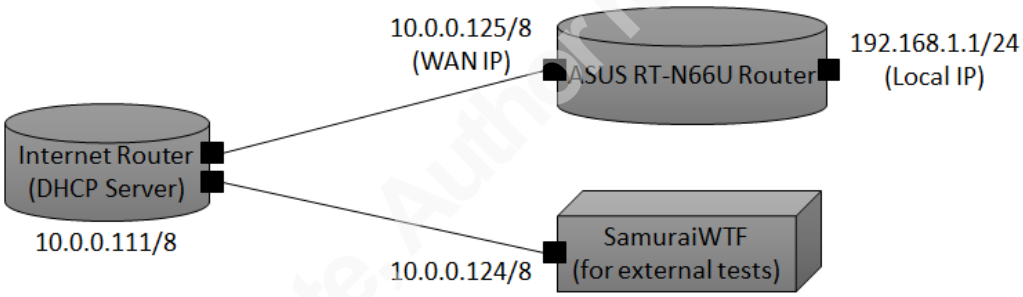

Figure 1 - Network diagram of test configuration

The following tools are used to perform the tests. They are all included in the SamuraiWTF distribution version 0.0.9 (Samurai Project, 2014):

- Nmap (version 5.00)
- cURL (version 7.18.2)
- Web browser (used Firefox 3.6.11)

Furthermore, the firmware version 3.0.0.4.352 is installed on the ASUS RT-N66U router as seen in Figure 2 - ASUS RT-N66U status page. The same figure shows a USB flash device connected to the router.

Figure 2 - ASUS RT-N66U status page

To simulate personal data stored on the connected USB device, a text file named "target_file.txt" with the content shown in Figure 3 - Target text file on USB device is stored on that device.

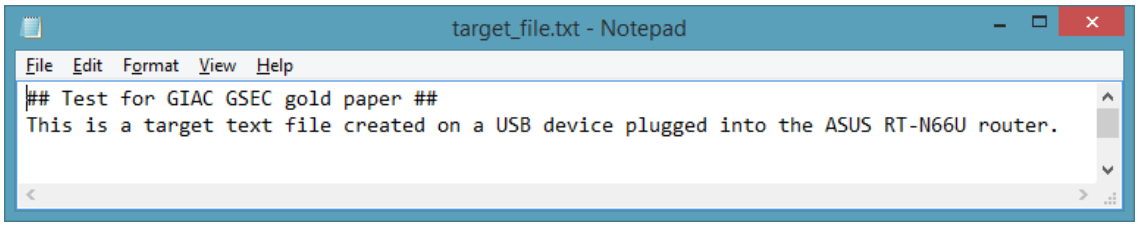

Figure 3 - Target text file on USB device

Christoph Eckstein, christopheckstein.sec@gmx.net

The final step in the test configuration is to activate the "Cloud Disk" service in the router's administration web interface.

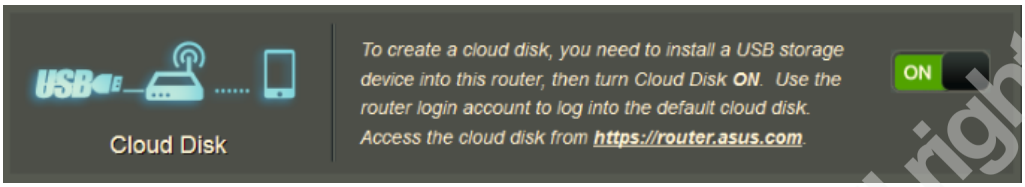

Figure 4 - Activate "Cloud Disk" option via the routers administration web interface

Activating "Cloud Disk" opens ports 443 and 8082 on the router's WAN interface. Port 443 is for AiCloud web access and port 8082 is for AiCloud content streaming. Except for the ports, the actual configuration of Cloud Disk and AiCloud is irrelevant to be able to exploit the vulnerability. Restricting access to specific users only will not impact the test configuration, as "authentication bypassing" implicates that no authentication is actually performed and no valid user credentials are needed.

3.2. Bypassing the authentication

All tests and commands in this section were run on the test system (IP address 10.0.0.124) against the WAN interface (IP address 10.0.0.125) of the ASUS RT-N66U router unless otherwise specified.

After setting up the test configuration, browsing to "https://10.0.0.125" shows the AiCloud login page as seen in Figure 5 - ASUS AiCloud login page. The router uses a self-signed SSL certificate to set up the encrypted connection over HTTPS. Therefore, the browser might detect an invalid certificate and display a warning notice, in which case the certificate must be manually accepted. The login page suggests that the data stored on the router and connected USB devices is only accessible after authenticating with valid login credentials.

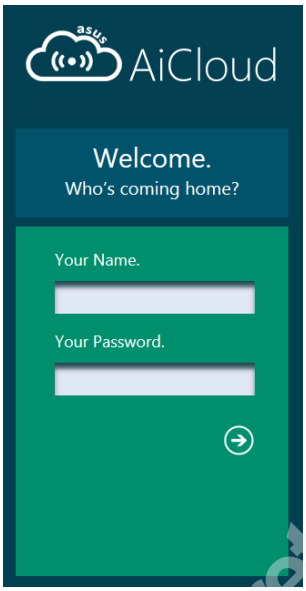

Figure 5 - ASUS AiCloud login page

A simple Nmap port scan shows open TCP ports 443 and 8082. This confirms the AiCloud configuration as seen on the router's administration web interface.

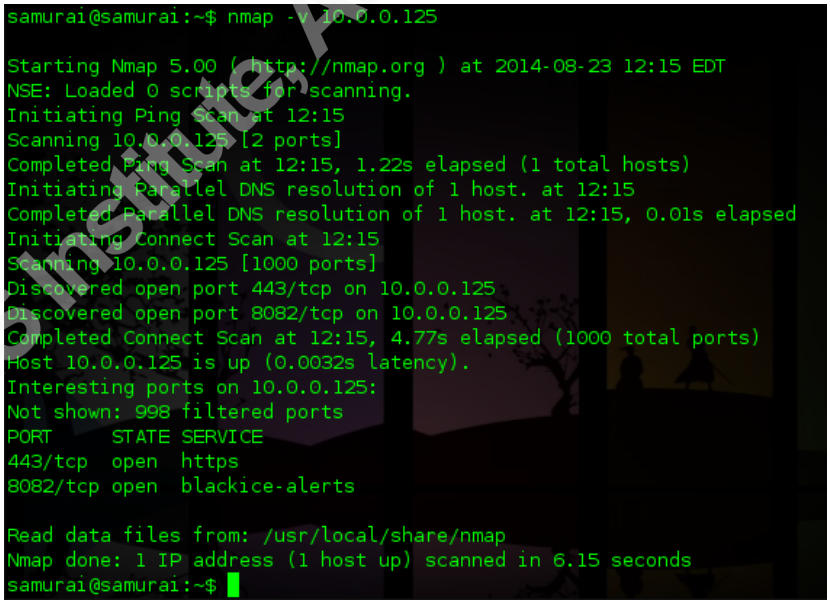

Figure 6 - Nmap port scan on external network interface

To demonstrate the vulnerability and read the content of the "target_file.txt" off the connected USB device, the following cURL command as shown in Figure 7 - Reading target_file.txt with curl over port 443 (HTTPS) is run.

```
curl https://10.0.0.125/smb/tmp/mnt/sda1/target_file.txt -k
```

The URL in this command directly points to the target file on the USB device mounted within the router's file system. The "-k" parameter instructs cURL to ignore self-signed or invalid SSL certificates. Otherwise the connection would fail and cURL would print a warning notice.

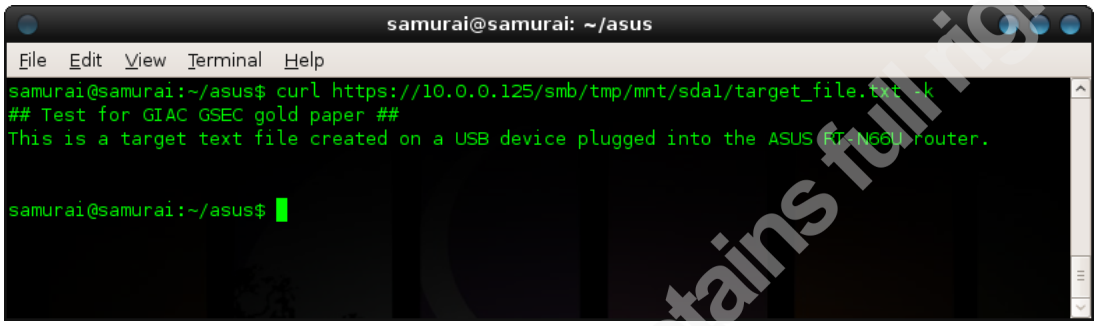

Figure 7 - Reading target_file.txt with curl over port 443 (HTTPS)

By running this simple command is it possible to directly access the router's file system and data stored on mounted external USB devices, even without providing any login credentials. This example illustrated the authentication bypass vulnerability in the ASUS RT-N66U router.

The same vulnerability is exploitable over TCP port 8082. The only difference is that simple HTTP without SSL is used.

```
curl http://10.0.0.125:8082/smb/tmp/mnt/sda1/target_file.txt
```

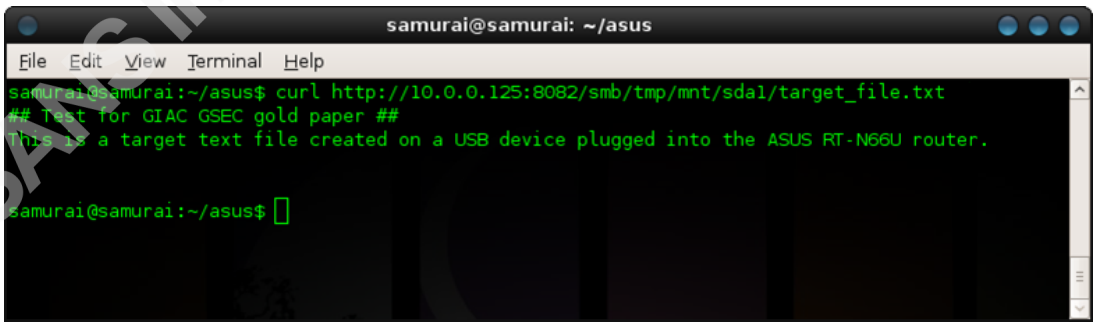

Figure 8 - Reading target_file.txt with curl over port 8082 (HTTP)

Furthermore, to download larger files or non-text files the curl "-o [output_file]" option could be used. This is useful to be able to further examine files on a local system, especially when encountering binary or encrypted files. Figure 9 - Downloading target_file.txt with cURL over port 443 (HTTPS) demonstrates downloading the

"target_file.txt" from the router's file system to the local file system. This is done by running the following command.

```
curl https://10.0.0.125/smb/tmp/mnt/sda1/target_file.txt -k -o
target_file.txt
```

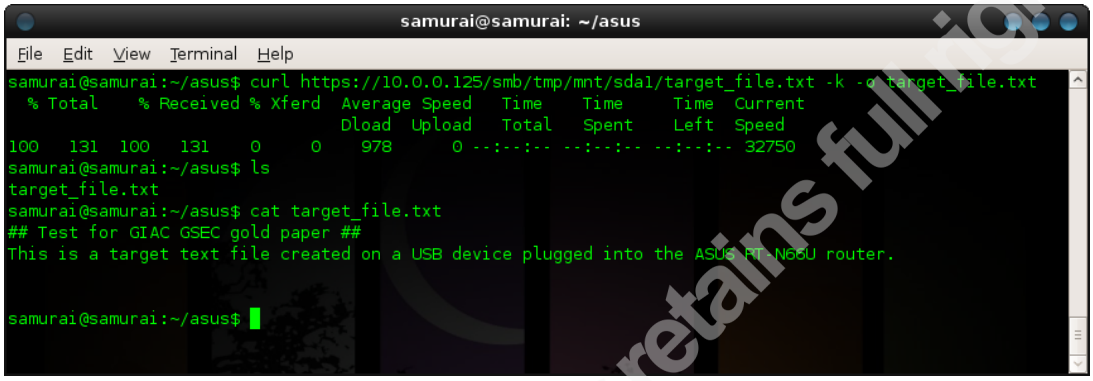

Figure 9 - Downloading target_file.txt with cURL over port 443 (HTTPS)

Further examining the router's file system even shows that critical system files are accessible via this authentication bypass. Figure 10 - Reading "passwd" file content with cURL and Figure 11 - Reading shadow file content with cURL illustrate reading the content of the "passwd" and "shadow" files on the router's file system.

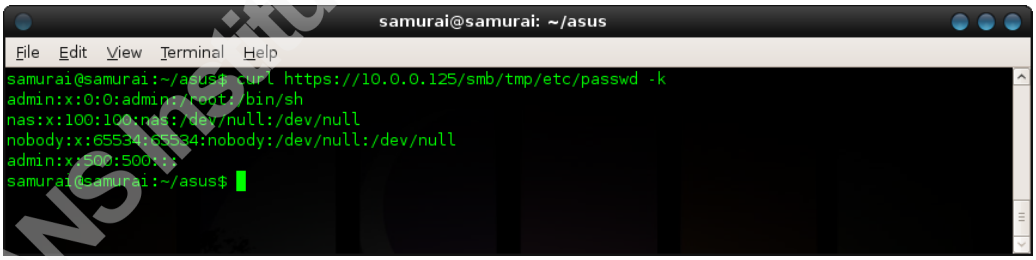

Figure 10 - Reading "passwd" file content with cURL

Being able to access both the "passwd" and "shadow" file, a malicious attacker can identify valid user account names listed within the "passwd" file. Furthermore, the shadow file provides the hashed passwords for these accounts. Depending on the complexity of the password chosen by the user, a malicious attacker might thereby be able to crack the passwords. If a malicious attacker is able to obtain a valid username and corresponding password, whilst remote administration of the router is enabled, he could potentially login to the administration interface and change the router's configuration.

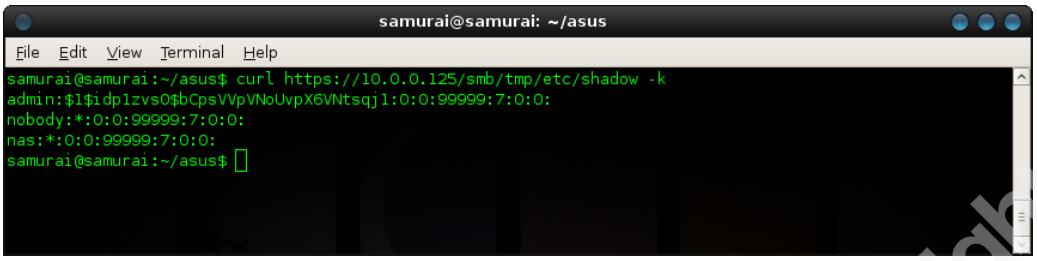

Figure 11 - Reading shadow file content with cURL

The same vulnerability can be exploited by simple browsing to the respective URL as shown in Figure 12 - Bypassing authentication and listing USB device content in Firefox.

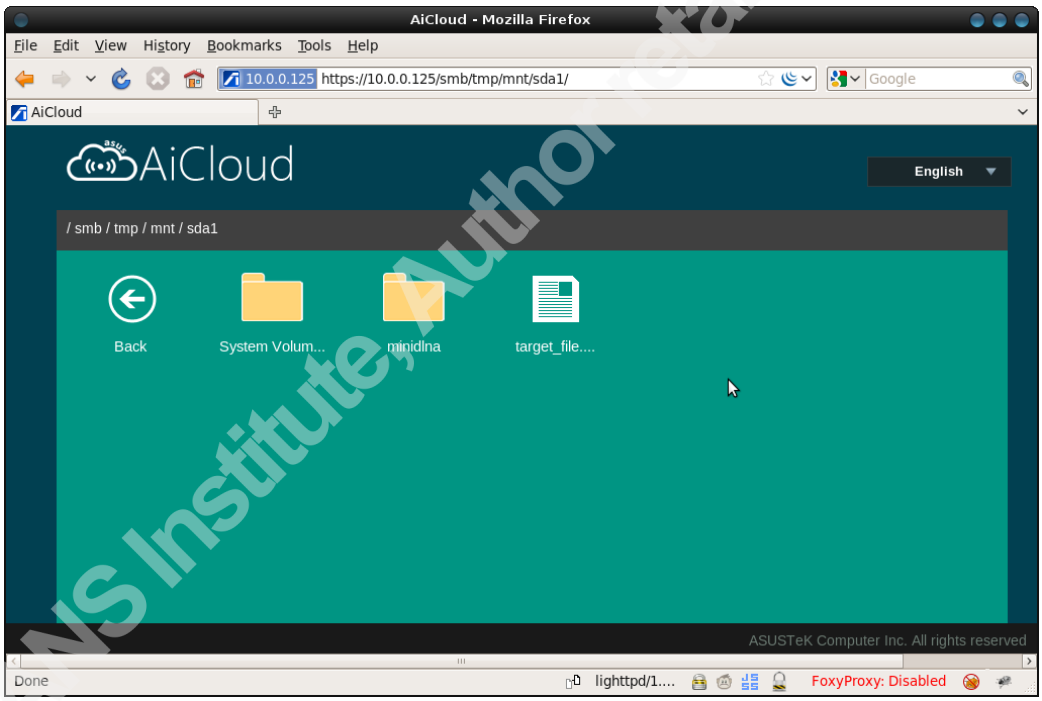

Figure 12 - Bypassing authentication and listing USB device content in Firefox

The authentication bypass vulnerability described above will work with any AiCloud option. When disabling “Cloud Disk” while enabling “Smart Access”, the exploit works the same way.

Christoph Eckstein, christopheckstein.sec@gmx.net

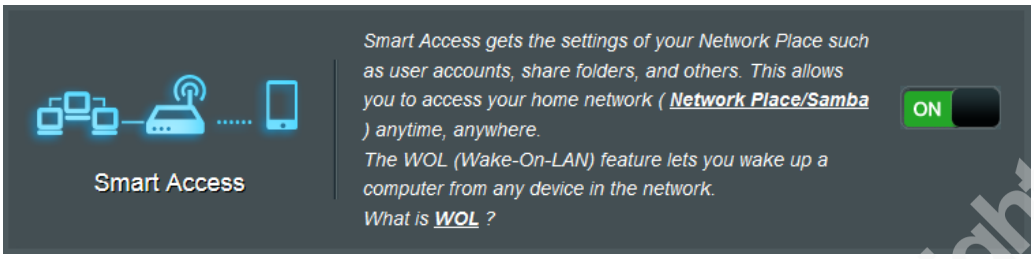

Figure 13 - Activate ASUS "Smart Access" in administration web interface

3.3. Vulnerability discovery

When doing web application penetration testing, one of the things to look for is unauthorized access to resources or directory traversal. In this case, simply looking at the login page source code gives a clue on what to look for. Figure 14 - HTML page source of the AiCloud login page shows the HTML source code of the login page. The resource links highlighted in the red rectangle are of interest. They seem to directly point at image files stored on the router's file system.

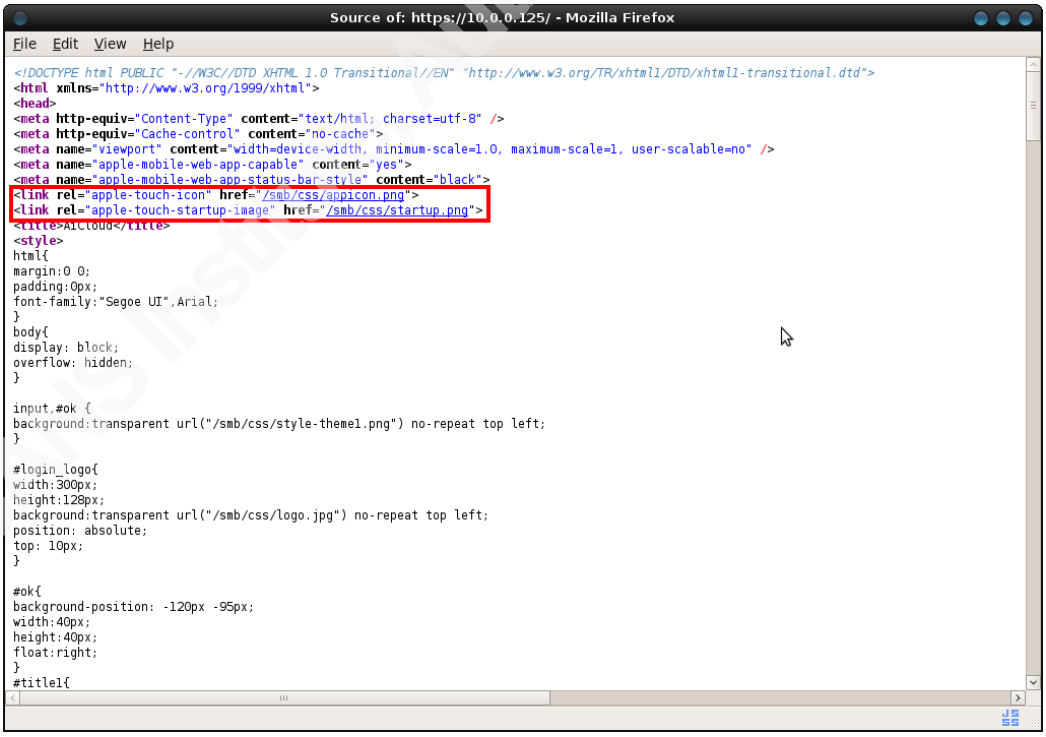

Figure 14 - HTML page source of the AiCloud login page

In this situation, it might be appropriate to say that a malicious attacker or web app penetration tester would try to see if other resources or folders might be directly accessible as well. This is called path traversal (OWASP Foundation, 2009). One

possibility might be too simple try if it is possible to list the content of overlying directories. This is demonstrated in Figure 15 – Bypassing authentication and listing the router's file system content in Firefox by browsing to the URL "https:10.0.0.125/smb/". This is a parent directory as seen in the resource URLs earlier. By browsing to this URL, the browser displays the directory structure of the router's file system without requesting any authentication. Being able to access the directory structure this way, it is relatively easy to enumerate the whole file system of the router by browsing through the folders.

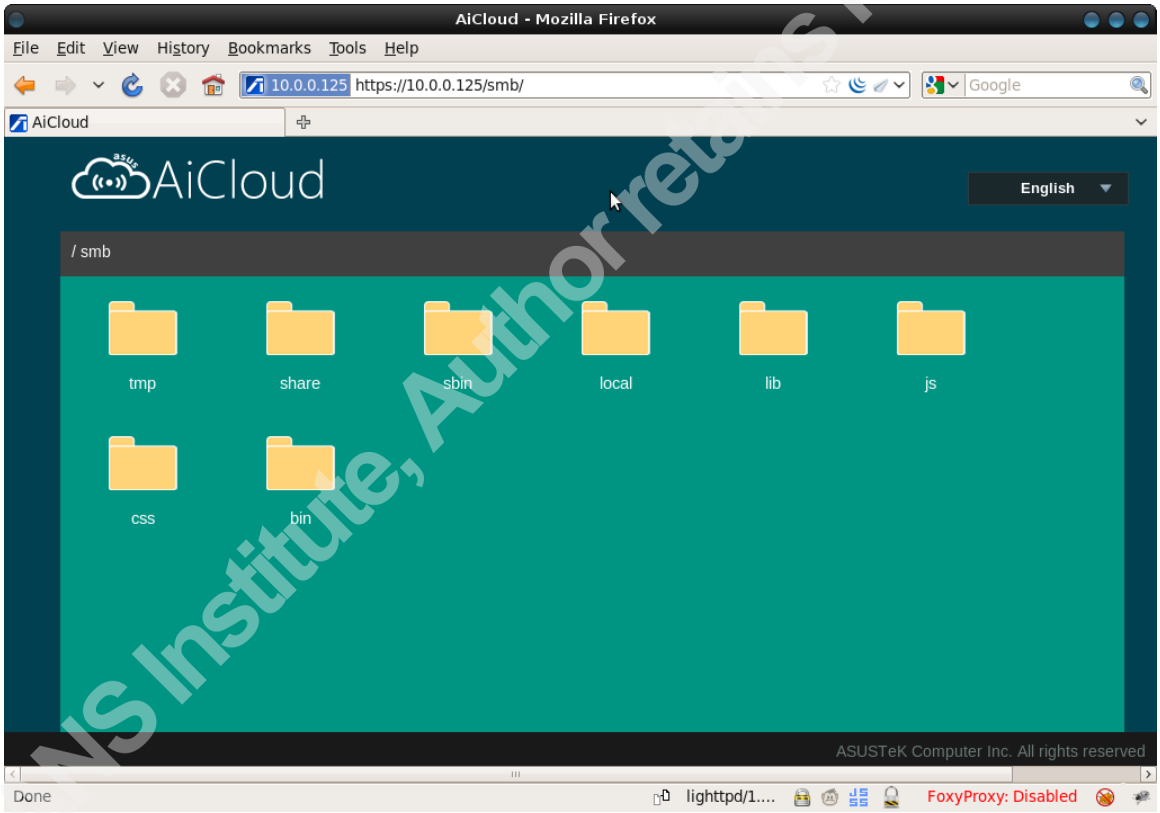

Figure 15 – Bypassing authentication and listing the router's file system content in Firefox

Through this basic test of simply trying to access resource folders used within the publicly accessible login page, the vulnerability can be discovered. The only option for users to mitigate this vulnerability is to completely disable AiCloud function on their router (Lovett, ASUS RT-N66U Router - HTTPS Directory traversal and full file access and credential disclosure vuln, 2013).

4. Can you trust your vendor?

The ASUS router backdoor example illustrates two mayor problems. First, new services like AiCloud are added to routers to improve user experience, but also introduce backdoors and security vulnerabilities. This indicates that vendors do not incorporate security into their development process and even neglect security testing and validation before distributing their products or new firmware. This becomes particularly apparent if considering that the previously demonstrated authentication bypass backdoor can easily be discovered with basic web application security testing. Secondly, in the example of ASUS, it took the vendor almost half a year to provide a fixed firmware version for their vulnerable products, which either left the user's personal data exposed or forced the users to implement other measures to mitigate the vulnerability (Kovacs, 2014). But the ASUS backdoor is just one example of many (Boose, 2014). An example for a purposely built-in backdoor is the so called "Joel's backdoor" in D-Link devices disclosed in October 2013 (Ducklin, D-Link router flaw lets anyone login through "Joel's Backdoor", 2013). Although D-Link released a fix within 6 weeks of the discovery, this case leaves the question of the purpose of the backdoor (Ducklin, D-Link patches "Joel's Backdoor" security hole in its SoHo routers, 2013). D-Link did not comment on any reason or cause. Ultimately, vulnerabilities in routers and network devices seem to be an overall concern with all mayor vendors (Boose, 2014). Some reports claim that even 80% of best-selling routers have security vulnerabilities (Gilbert, 2014). Almost any router shows vulnerabilities that lead to unauthorized access to the router and thereby personal data stored on connected storage devices (Independent Security Evaluators, 2013). This puts the vendors' development process into question. Studies show various deficits in router development processes regarding security (Antipolis, 2014). A good example for this is the discovery of default admin passwords in Cisco devices in 2006 (Cisco Systems, Inc., 2006). Such negligence in the development process undermines the overall security of such devices.

Furthermore, vulnerabilities in routers do not only put personal data on storage devices at risk, but also endanger the privacy and control of private networks. With the increasing reports of malware explicitly targeting routers and network devices, how can users make sure they keep control of their private networks? Malware like the IOS Trojan

discovered in 2009 (Peláez, 2009) or even self-replicating worms like "The Moon" for Linksys devices discovered in 2014 (Ullrich, 2014) potentially may take over the control of routers and network devices. Once in control, there possibilities to cause harm could be without limits. Without even knowing they could open additional backdoors for malicious attackers, they could be used as staging points for further attacks or they could be turned into bots. Likewise, they could be used to stage man-in-the-middle attacks or reroute DNS traffic in order to eavesdrop on potentially encrypted private connections. This would not only disclose our private data in transit, but malicious attackers could also intercept online banking connections and gain access to personal accounts (Goodin, Bizarre attack infects Linksys routers with self-replicating malware, 2014).

Regardless of the amount of vulnerabilities found, vendors could be expected to quickly fix vulnerabilities as soon as they are disclosed. But the example of ASUS taking half a year to make an official fix available proves reality to be quite the opposite. Furthermore, vendors not always seem to fix vulnerabilities thoroughly enough, leaving devices just as vulnerable as they were beforehand (Scherschel, 2014). Reports of Cisco stating to have fixed a vulnerability, but actually just having disguised it may even suggest that vendors intentionally built in backdoors and hope to keep them hidden without intentions to fix them. (Previous Contributors, 2014)

With all these vulnerabilities and reports, can users trust their vendor to build secure routers and network devices? And furthermore, what can they do to protect their personal data if they cannot rely on the security of their routers?

5. Securing your router

If users cannot rely on the vendor to provide us with secure network devices straight out-of-the-box, they have to take additional steps to secure their network perimeter. These steps include validating vendor hardware to make sure it is secure and properly configured. But despite all precautions, there is no guarantee there will be no vulnerabilities discovered at some point later on. With the complexity of devices and evolving methods of malicious attackers it becomes more and more difficult to test and validate every possible (and future) attack vector against a device. This becomes even

more apparent when considering the resources and knowledge that are needed for such tests. For smaller organizations and private homes this may be too expensive and not cost effective. Thus, users also have to add additional layers of defense to prepare for one being prawn to fail. This is also known as defense-in-depth.

5.1. Detecting backdoors

An ideal approach for detecting backdoors would be to fully test and validate the security of a router before putting it into production. Users should perform some kind of evaluation before purchasing a new router. But due to limited resources, time and budget for this evaluation process, users often limit their evaluation to criteria like functionality and performance. However, the ASUS router authentication bypass example shows that basic security testing of the AiCloud web application by a professional web application penetration tester could have identified the vulnerability. Users, especially organization, might be well advised to perform at least some basic security testing on new devices.

Depending on the desired security level of a router, organizations should incorporate security requirements and tests into an evaluation process before purchasing new devices. Such tests may include vendor documentation review or automated testing for common vulnerabilities. This is especially recommended for any internet-facing web interface provided by a router. Additionally, manual testing could be useful, although this may require deeper technical knowledge and skills. Manual testing can include source code analysis of firmware (The Trail of Bits Team, 2014) and extensive penetration testing. There are even interesting projects that seek automate firmware analyses, but these are not part of this paper (The Firmware.RE Team, 2014). And if users don't have access to the actual source code, there are still methods to identify hidden backdoors via string analysis (Santamarta, 2013).

Even after extensive testing, there might still be unknown backdoors or vulnerabilities in a router. Therefore, penetration tests should be done periodically. Continuous test are not only useful to adapt new testing methods, but also to make sure no backdoors are created by changing configuration settings or applying updates. Basic tests to ensure no ports were opened due to configuration changes may use publicly available scanning tools like "ShieldsUp!" (Gibson Research Corporation, n.d.). More

advanced techniques include behavior monitoring and evaluation to detect potential backdoors and information disclosure (Zhang & Vern, 2000). In reality, performing penetration tests on their own network devices would be ideal, but if organizations lack dedicated security personnel, they may not view this activity as practical. Nonetheless, the least organizations should do is scanning the outside interface of their network for unknown open ports and monitoring vendor advisories for vulnerability disclosures. An exceptional organization will also monitor newsgroups, twitter and popular blogs for additional info.

But finally, one problem remains. What can be done if a potential backdoor or vulnerability in a router is detected? An immediate shut down might potentially impact the organizational capability to run its main (business) processes. One option may be temporary deactivating any services or options that cause the backdoor or vulnerability. In any case, the safest solution is to fix and upgrade the router's firmware, but this vastly depends on the vendor's ability and often willingness to provide a fixed firmware version in a timely manner.

5.2. Changing default configurations

Another vulnerability discovered in ASUS routers concerning the FTP service illustrates a problem with default configurations. By default, when activated, the FTP service allowed anonymous access with full access rights. The user first had to manually add a FTP user to disable anonymous access, but there were no instructions for the user to indicate this (Lovett, ASUS RT Series Routers FTP Service - Default anonymous access, 2014). ASUS has fixed the vulnerability by simplifying the configuration options (Ricknas, 2014). Nevertheless, this example demonstrates that users should check and change the default configuration of their routers to prevent such vulnerabilities. One approach to default configurations is to first deactivate any unused services and configuration options, and incrementally enable and configure them as needed. This is especially useful as multitude of extra services added to modern routers may introduce new attack vectors, although most users may only use a fraction of all these services (Independent Security Evaluators, 2013).

Before deploying new network devices or routers, their configuration should be checked and validated. Similar to operating systems, unneeded services should be disabled, default passwords should be changed, and security options should be reviewed to be set to the best available standards. Furthermore, when configuring network devices, communication should encounter over a secure connection. Most modern routers offer HTTPS webpages for configuration, although the default configuration might be set to use HTTP without encryption.

Various hardware vendors, e.g. Cisco, offer useful hardening guides for their devices (Singh, 2014). Additionally, the System and Network Attack Center offers great resources on how to securely configure routers and network devices (System and Network Attack Center (SNAC), 2005). There are even guides that specially focus on IPv6 (Router Security Configuration Guide Supplement - Security for IPv6 Routers, 2006).

5.3. Defense-in-depth

In the end, one security measure, or router in this case, could not provide 100% security for users. Fact is that any single security mechanism will fail; a backdoor or other vulnerability will be discovered at some point in time. It is impossible to ultimately prevent or detect hidden or involuntary backdoors in ever more complex devices. To be prepared for a possible backdoor or vulnerability, a defense-in-depth approach has to be considered. Such an approach does not rely on one security mechanisms or systems; it rather implements a series of security mechanisms with the assumption for one of these to fail without compromising the security of the whole system. (Small, 2011). Furthermore, if several security devices are from the same vendor, one vulnerability in the firmware might affect all devices. This should be taken into account when setting up defense-in-depth.

6. Building more secure routers

Despite all the different measures to secure routers outlined so far, it is the vendors' responsibility to build and maintain their devices and ensure they are secure. Although it is possible to set up custom routers (Bothwick, 2010) or to install unofficial

firmware available for vendor devices (Hoffman, 2014), organizations most likely rely on official patches and support of vendors. Especially as unofficial patches come with their own security concern if the creator is unverified.

6.1. Secure router development

To build more secure routers, hardware vendors have to adopt a more security-focused development process. Security should be implemented into the design to conform to newest security principles and standards. Best practices like "least privilege" and "secure by default" should be followed, as it is common practice in software development (Independent Security Evaluators, 2013). For instance, the previously shown ASUS RT-N66U vulnerability could have been avoided by strict quality and security controls throughout the development process. Web application developments guides and test, such as proclaimed by OWASP for example, should be adopted for router web services likewise (OWASP Foundation, 2009).

Cisco has published their "Cisco secure development lifecycle" (Cisco Systems, Inc., 2014), as well as other podcast on secure development (Johnston, White Jr., Romeo, & Meyers McDonald, 2014). Nonetheless, vulnerabilities and even default admins passwords were discovered on Cisco devices (Cisco Systems, Inc., 2006). Additionally, even the best secure development processes are undermined by purposely implemented hidden backdoors (Craig, 2013).

6.2. Managing router updates

There is another challenge related to the ASUS example. Although ASUS did make a security fix available after some time, many router are still vulnerable. Despite all reports of the severity of the vulnerability, users fail to apply the corresponding patch (Rosenblatt, Asus router vulnerabilities go unfixed despite reports, 2014). It shows that there is a need to rethink the way router updates are performed. As of now, users have to manually download the firmware from the vendors' homepage or to manually start the update routine within their routers administration interface. Therefore, there is a need to provide a more automated and secure way to distribute firmware updates to devices. Some sort of auto-update function like in modern operating systems and even web browsers today would be nice to have (Rosenblatt, Top Wi-Fi routers easy to hack, says

study, 2013). Just fixing the vulnerability and releasing a new firmware version does not consequently solve the problem. To increase user confidence in the security of devices at any time vendors will have to quickly respond with security fixes and incorporate some sort of update mechanism to deliver them without manual user interaction.

7. Conclusion

Research and reports indicate that security might not be a primary focus of router vendors. Out-of-the-box routers come with various vulnerabilities and backdoors, including basic authentication bypass vulnerabilities as shown in the example. Constantly adding new services and functionality to their products, vendors introduce even more vulnerabilities and attack vectors (Independent Security Evaluators, 2013). Furthermore, reports indicate that vendors purposely built in backdoors. Additionally, some vendors take their time to provide security fixes and patches after vulnerabilities are disclosed, leaving users on their own to find temporarily mitigations. All this substantiates the argument whether users can trust vendors to ensure the security of their personal data; especially in the case that vendors try to hide backdoors after disclosure instead of effectively fixing it.

To mitigate the risk of router backdoors users have to thoroughly test routers before deployment. Basic steps include checking default configurations to make sure no unneeded or potentially insecure remote services are activated and default accounts are changed. Additionally users will have to prepare for the event of a possible security break within their routers with a defense-in-depth approach. After all, there is no guarantee that any security mechanism will prevail. In fact, given enough resources and time a malicious attacker will circumvent any security mechanism (Information Assurance Solutions Group, 2014). Defense-in-depth seems even more necessary with the amount of vulnerabilities found in routers nowadays. Another important part is to keep up-to-date with vulnerability disclosures and security incidents. Knowing what vulnerabilities and exploits are currently present, and how to temporarily mitigate the risk associated with them until a patch becomes available is essential for users to secure their routers and personal data (Todd, 2003). Ultimately, unless users want to build their own routers or install invalidated third-party patches, vendors will have to provide more secure products.

Christoph Eckstein, christopheckstein.sec@gmx.net

Vendors will have to improve their development processes to offer more secure products and to make security fixes and patches available faster after a vulnerability disclosure. They have to incorporate security as a key design feature in their products. On the other hand, even if vendors implement security fixes and patches in a timely manner, user will still have to stay informed and download and install patches manually. So just improving the development of their devices and firmware patches is not enough for vendors. They will have to design more practical and automated update mechanisms to ensure patches are applied to vulnerable devices.

The reality is that users will have to wait and see whether vendors will improve their development processes and provide more secure products out-of-the-box. In conclusion it can be said that future research and reports will have to show if vendors will incorporate security as a key feature of their products, and whether vendors will come up with practical and automated mechanism to apply security fixes and patches to devices out in the field. By doing so, vendors will eventually be able to raise the trust and confidence of users in the security of their products.

Christoph Eckstein, christopheckstein.sec@gmx.net

8. References

Antipolis, S. (2014, 08). *A Large-Scale Analysis of the Security of Embedded Firmwares.* Retrieved 08 20, 2014, from http://www.s3.eurecom.fr/docs/usenixsec14_costin.pdf

ASUSTeK Computer Inc. (2014). *AiCloud*. Retrieved 08 24, 2014, from http://event.asus.com/2012/nw/aicloud/

Boose, S. (2014, 02 24). *MAJORITY OF SOHO WIRELESS ROUTERS HAVE SECURITY VULNERABILITIES*. Retrieved 08 05, 2014, from http://www.tripwire.com/state-of-security/top-security-stories/majority-soho-wireless-routers-security-vulnerabilities/

Bothwick, N. (2010, 12 28). *How to build your own router*. Retrieved 09 03, 2014, from http://www.techradar.com/news/networking/how-to-build-your-own-router-915419

Cisco Systems, Inc. (2006, 01 11). *Default Administrative Password in Cisco Security Monitoring, Analysis and Response System (CS-MARS)*. Retrieved 08 07, 2014, from http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060111-mars

Cisco Systems, Inc. (2014). *Cisco Secure Development Lifecycle (CSDL)*. Retrieved 07 30, 2014, from http://www.cisco.com/web/about/security/cspo/csdl/index.html

Cisco Systems, Inc. (2014, 06 02). *Multiple Vulnerabilities in Cisco NX-OS-Based Products*. Retrieved 08 05, 2014, from http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-nxos

Craig. (2013, 10 12). *Reverse Engineering a D-Link Backdoor*. Retrieved 08 20, 2014, from http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/

DefenseCode Security Advisory. (2013, 01 15). *Broadcom UPnP Remote Preauth Root Code Execution.* Retrieved 08 04, 2014, from http://www.defensecode.com/public/DefenseCode_Broadcom_Security_Advisory.pdf

Ducklin, P. (2013, 12 03). *D-Link patches "Joel's Backdoor" security hole in its SoHo routers*. Retrieved 07 30, 2014, from

http://nakedsecurity.sophos.com/2013/12/03/d-link-patches-joels-backdoor-security-hole-in-its-soho-routers/

Ducklin, P. (2013, 10 15). *D-Link router flaw lets anyone login through "Joel's Backdoor"*. Retrieved 07 30, 2014, from http://nakedsecurity.sophos.com/2013/10/15/d-link-router-flaw-lets-anyone-login-using-joels-backdoor/

Gibson Research Corporation. (n.d.). *Welcome to ShieldsUP!* Retrieved 08 14, 2014, from https://www.grc.com/shieldsup

Gilbert, D. (2014, 02 21). *80% of Best-Selling Wireless Routers Have Security Vulnerabilities*. Retrieved 08 04, 2014, from http://www.ibtimes.co.uk/80-best-selling-wireless-routers-have-security-vulnerabilities-1437458

Goodin, D. (2013, 01 24). *Secret backdoors found in firewall, VPN gear from Barracuda Networks*. Retrieved 08 05, 2014, from http://arstechnica.com/security/2013/01/secret-backdoors-found-in-firewall-vpn-gear-from-barracuda-networks/

Goodin, D. (2014, 02 13). *Bizarre attack infects Linksys routers with self-replicating malware*. Retrieved 08 07, 2014, from http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/

Hoffman, C. (2014, 05 13). *How to Use a Custom Firmware on Your Router and Why You Might Want To*. Retrieved 09 16, 2014, from http://www.howtogeek.com/189073/how-to-use-a-custom-firmware-on-your-router-and-why-you-might-want-to/

Independent Security Evaluators. (2013, 07 26). *SOHO Network Equipment.* Retrieved 08 13, 2014, from https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf

Information Assurance Solutions Group. (2014). *Defense in Depth.* Retrieved 09 03, 2014, from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Johnston, J., White Jr., D., Romeo, C., & Meyers McDonald, L. (2014, 05 05). *The Cisco Secure Development Lifecycle*. Retrieved 07 30, 2014, from

http://www.cisco.com/c/en/us/solutions/enterprise-networks/security/security_tac_podcasts.html

Kirk, J. (2013, 10 14). *Backdoor found in D-Link router firmware code*. Retrieved 09 16, 2014, from http://www.itworld.com/data-protection/378427/backdoor-found-d-link-router-firmware-code

Kovacs, E. (2014, 02 13). *ASUS Fixes Vulnerabilities in RT-N66U, RT-N66R and RT-N66W Routers*. Retrieved 08 28, 2014, from http://news.softpedia.com/news/ASUS-Fixes-Vulnerabilities-in-RT-N66U-RT-N66R-and-RT-N66W-Routers-426689.shtml

Lovett, K. (2013, 06 22). *ASUS RT-N66U Router - HTTPS Directory traversal and full file access and credential disclosure vuln*. Retrieved 08 26, 2014, from http://www.securityfocus.com/archive/1/526942

Lovett, K. (2014, 02 12). *ASUS RT Series Routers FTP Service - Default anonymous access*. Retrieved 08 13, 2014, from http://www.securityfocus.com/archive/1/531046/30/0/threaded

OWASP Foundation. (2009, 05 27). *Path Traversal*. Retrieved 08 26, 2014, from https://www.owasp.org/index.php/Path_Traversal

Peláez, M. H. (2009, 08 04). *IOSTrojan: Who really owns your router?* Retrieved 07 30, 2014, from http://www.sans.org/reading-room/whitepapers/malicious/iostrojan-owns-router-33324

Previous Contributors. (2014, 04 22). *Router Backdoors Were Hidden – Never Patched*. Retrieved 08 27, 2014, from http://www.tripwire.com/state-of-security/top-security-stories/router-backdoors-were-hidden-never-patched/

Ricknas, M. (2014, 01 13). *Asus simplifies router configuration to protect external hard drives*. Retrieved 08 13, 2014, from http://www.networkworld.com/article/2173358/byod/asus-simplifies-router-configuration-to-protect-external-hard-drives.html

Rosenblatt, S. (2013, 04 17). *Top Wi-Fi routers easy to hack, says study*. Retrieved 08 13, 2014, from http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/

Rosenblatt, S. (2014, 02 18). *Asus router vulnerabilities go unfixed despite reports*. Retrieved 08 13, 2014, from http://www.cnet.com/news/asus-router-vulnerabilities-go-unfixed-despite-reports/

Router Security Configuration Guide Supplement - Security for IPv6 Routers. (2006, 05 23). Retrieved 08 05, 2014, from http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf

Samurai Project. (2014). *Samurai Web Testing Framework*. Retrieved 08 23, 2014, from http://samurai.inguardians.com/

Santamarta, R. (2013, 05 23). *Identify Backdoors in Firmware By Using Automatic String Analysis*. Retrieved 08 25, 2014, from http://blog.ioactive.com/2013/05/identify-back-doors-in-firmware-by.html

Scherschel, F. (2014, 06 03). *Huawei-Router lassen sich aus dem Internet kapern*. Retrieved 08 04, 2014, from http://www.heise.de/security/meldung/Huawei-Router-lassen-sich-aus-dem-Internet-kapern-2214983.html

Singh, S. (2014, 06 03). *Cisco Guide to Harden Cisco IOS Devices*. Retrieved 08 05, 2014, from http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Small, P. E. (2011, 11 14). *Defense in Depth: An Impractical Strategy for a Cyber World.* Retrieved 08 25, 2014, from http://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896

System and Network Attack Center (SNAC). (2005, 12 15). *Router Security Configuration Guide.* Retrieved 08 05, 2014, from http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf

The Firmware.RE Team. (2014). *Firmware.RE*. Retrieved 08 25, 2014, from http://firmware.re/

The Trail of Bits Team. (2014). *CTF Field Guide*. Retrieved 08 14, 2014, from http://trailofbits.github.io/ctf/

Todd, A. H. (29. August 2003). *Vendor-Supplied Backdoor Passwords - A Continuing.* Abgerufen am 13. 06 2014 von http://www.sans.org/reading-room/whitepapers/awareness/vendor-supplied-backdoor-passwords-continuing-vulnerability-32899

Christoph Eckstein, christopheckstein.sec@gmx.net

Ullrich, J. (2014, 02 13). *Linksys Worm "TheMoon" Summary: What we know so far*. Retrieved 07 30, 2014, from https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633

Zhang, Y., & Vern, P. (August 2000). *Detecting Backdoors.* Abgerufen am 13. 06 2014 von http://www.icir.org/vern/papers/backdoor-sec00.ps.gz

Christoph Eckstein, christopheckstein.sec@gmx.net