ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
«ADSL Router Exploitation»

Αναστάσιος Στασινόπουλος (ΑΜ: MTE1225)

Επιβλέπων Καθηγητής :
Χρήστος Ξενάκης

Table of Contents

Abstract

ADSL routers are an integral part of today's home and small office networks. Typically, these devices are provided by a user's ISP and are, usually, managed by people who do not have any special technical knowledge. Often poorly configured and vulnerable, such devices are an easy target for network-based attacks, allowing cyber-criminals to quickly and easily gain control over a network. In this paper, we systematically evaluate the security of ADSL routers and identify the potential of attacks, which attempt to compromise the vulnerabilities of their web interface.

More specifically, we present common vulnerabilities and attacks that occur in websites on the Internet, and project them on the special characteristics of the web management interface of ADSL routers. To put this analysis into a practical context, we investigate the security of a popular ADSL router provided by a Greek ISP.

In this security assessment, we have discovered two 0-day vulnerabilities in the web management interface of the tested router. In particular, we discovered an operating system (OS) command injection and stored Cross-Site Scripting (XSS) attack.

A malicious may exploit these vulnerabilities to perform several large-scale attacks. Specifically, he/she can perform DNS hijacking attack and redirect the users to fake web sites for phishing; mount a Distributed Denial of Service (DDoS) attack using the compromised routers as zombie machines; or even spread a malware. Finally, we discuss some well-known security practices that should be followed fro

1. Introduction

In recent years, there has been a significant increase in broadband Internet access in Greece. According to the Hellenic Telecommunications & Post Commissions, the penetration of broadband Internet access in June 2012 has reached 2.560.414 subscribers (22.6% of the total population of Greece) [1].

There are seven major ISP operating in Greece, such as OTE Conn-X, Forthnet, Hellas On Line, WIND Hellas, Cyta hellas, On Telecoms and Vodafone Hellas. At the time of a new subscription, the ISP provides, freely, an ADSL router to their customers. The ADSL router is the most important part in a SoHo (Small Office / Home Office) network, since it controls the traffic flow between the Internet and the internal network. It includes a web-based administration interface, which can be accessed through a log-in process using a browser.

Although this web interface is an effective solution from a usability point of view, it is an Achilles' heel in terms of security and the overall system's robustness. Having acknowledged this, some individual security activists have investigated the security of many popular ADSL routers, and proceeded in publishing their finding as well as the discovered vulnerabilities, mainly, in a form of exploits [3] [4] [5] [6] [7].

Moreover, a collective study of vulnerabilities, discovered in the web interface of embedded devices, was presented in [13]. This satisfies the objectives of activists and may facilitate the manufactures and ISPs to patch the security holes of their products; but it is not fruitful in understanding the reasons why these weaknesses continue to occur, and what will be the impact of a possible attack that exploit such vulnerabilities.

This is the motivation of this paper, which attempts to fill the above mentioned gap in an holistic and technically sound approach by:

1. Discussing the basic weaknesses that occur at ADSL routers.

2. Presenting a manual methodology (not an automated one) that we have followed to investigate the security of an ADSL router.

3. Analyzing the impact of the discovered vulnerabilities.

4. Presenting some well-known security practices that should be followed during routers implementation and usage.

In general, the security holes of ADSL routers are attributed due to the poorly written software of these devices.

It also seems that the ISPs are not aware of the security impacts and harm that these vulnerabilities may cause. Recently, it was discovered that several Brazilian ISPs have fallen victims of a series of domain name system (DNS) hijacking attacks, which compromised a whopping number of 4.5 million ADSL routers [2].

The attack exploited a security hole in the routers' web interface, which allowed a Cross Site Request Forgery (CSRF) to be performed in their administration panel, allowing the attacker to make changes in the DNS servers. Once compromised, users were redirected to specially crafted phishing domains that mainly targeted users' online banking credentials.

Another security issue of the ADSL routers has to do with the fact that once installed and configured, end-users will probably overlook to update their firmware, since it is a manual and tedious process. Moreover, many home users simply do not have any technical knowledge to perform software updates in the ADSL routers.

Thus, even if the vendor of a vulnerable router releases, eventually, a security patch, it will not be applied in many devices. In this paper, we systematically evaluate the security of ADSL routers and identify the potential of attacks, which attempt to compromise the vulnerabilities of their web interface. More specifically, we present common

2. Understanding the risk of threats

Often network equipment devices such as ADSL routers, printers and similar equipment are forgotten (about applying firmware updates) once installed and configured. The ADSL router is the most important part in a SoHo network, controls the flow of traffic between the Internet and the internal SoHo network hosts through a web-based administrative interface.

It is really disturbing that the most important part of the SoHo network may be vulnerable to web-based (severs-side either client-side) attacks such us. Like most embedded devices so in the case of ADSL routers, the web interface is written in programming languages such as HTML, PHP, PERL (combined with CGI scripts) etc.

The incorrect programming of these applications can cause the same problems that encountered on websites. Unfortunately, along with the ease of writing the code of applications -that will be used on the interface of the router- such programming languages bequeath vulnerabilities they have. In our view, those applications should be treated in the same way they would be treated as a web application and will probably suffer from the same vulnerabilities.

The attacks that could occur in ADSL routers are divided into two categories: server-side and client-side attacks. Server side attacks target the router aiming at altering its normal behavior or disclosing sensitive information, such as root passwords. On the other hand, client-side attacks target an unsuspecting user connected to the ADSL router. This type of attacks is triggered by an end-user action using a browser, which interacts with a compromised or malicious web site, forcing it to execute malicious code or process data.

2.1 Server-Side Attacks

Servers exposes a lot of services that clients can interact with. As a server exposes services, it exposes potential vulnerabilities that can be attacked. Merely running a server puts oneself at risk, because a hacker can initiate an attack on the server at any time. For example, an attacker could send a maliciously crafted HTTP request to a vulnerable web server and attempt to leverage errors or other unexpected application behavior

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.

2.1.1 Authentication bypass Attacks

Through authentication bypass attacks, an attacker is able to bypass user authentication mechanisms that the web interface of the ADLS router uses for the administration and management on ADSL router device. Successful authentication bypass discloses sensitive information and allows execution of arbitrary commands with administrative privileges.

Most of the security holes found on the web interface of embedded devices, which may lead to authentication bypass, fall into one of the following categories:

1. Multiple representation of valid URLs.
2. Knowledge of “post-authentication” URLs .
3. Unchecked HTTP methods .
4. Unprotected cgi scripts .

In the first category, an attacker tries to find alternative ways to represent a URL that would grant access to administration functionality. That is, there are multiple ways that a URL can be represented, where it is still valid by the web application, without the latter requesting from the user to enter the username and password.

This happens because developers do not filter and validate properly the URLs that a web application receives. Therefore, the web application may accept multiple representations of the same URL as valid, without requiring authentication.

For example, assume that the URL for accessing the firewall settings is “http://homehub/cgi/b/firewall/” and requires an admin account username and password.

The attacker can try the following alternatives for the above URL that may provide access to the firewall settings, without however requiring the administrator password.

- http://homehub/cgi/b/firewall/%5C
- http://homehub/cgi/b/firewall//
- http://homehub/cgi/b/firewall/~
- …

In the second category, the attacker exploits the following functionality common in many routers: when accessing a web interface of an appliance, the user is prompted to enter a password. Once, the admin user enters his/her username/password, the device verifies whether the provided credentials are valid. After a successful authentication, the web application reveals hidden URLs that are used for administration functionality.

The problem stems from the fact that the authentication mechanism of some routers is so weak, that when an unauthenticated user requests a hidden URL, the web application does not ask for a password and delivers the hidden web page to the unauthenticated user. One may argue that this attack cannot be performed, because an unauthenticated user cannot know the hidden URL paths to access the related hidden web pages.

However, this assumption is erroneous, because there are many ways that an attacker can discover hidden URLs. For example, the attacker can perform directory bruteforcing (i.e., try randomly various possible combinations of URLs) [14], since the URL paths are very easy to guess. To rectify this erroneous functionality, the web application should use session identities to check for each single HTTP request whether the user is in fact authenticated.

In the third category, the ADSL router performs an authentication check, only, when a request is performed using a certain HTTP method. In this case, the attacker can simply change the HTTP method from GET to POST or vice versa and gain access to the administrator's functionality. Finally, in the fourth category, the authentication bypass is due to the following case.

Many web applications use CGI scripts to process input data and generate dynamic content. In this case, authentication bypass can be performed because the web pages correctly accept HTTP requests only from authenticated users, but the respective CGI script, which performs the actual processing of the request, does not require an authenticated request. This happens because the developer overlooked the fact that CGI scripts should also perform validation of HTTP requests.

2.1.1.1 Default Credentials (Username/Passwords)

Several (mostly home) users who are not familiar with computer security, neglect to change the ADSL router vendor's default credentials (username / password). On the Internet there are many sites such as the "Routerpasswords.com" [2] who maintain databases stored there default credentials on several well-known ADSL router vendors around the world.

Usually, vendors use the same or similar passwords across different models so it's quite easy for an attacker to guess credentials in an ADSL router, where the administrator has not taken care to change them.

In a survey that we did in a Greek company “OTE Conn-X” we found that on “Conn-x BaudTec” routers devices series T263R* and TW263R*, the administrator's account has by default user-name "admin" with no option either from inside the administration panel for change.

The default administrator's password is depending on the model of the router. Is important to mention that the default password for the administrator's account is often left on without being changed. Default password for administrator's account on T263R1U* router series account is "1234".

In the case of T263R4* routers series the default password is 12 digits and is written on the sticker underneath the modem named as "MAC". For example if mac address of the router is "00:13:33:1D:DD:62" the administrator's default password would be "0013331ddd62".

2.1.1.2 Unauthorized Information Disclosure Attacks

Due to access control errors, unauthorized information disclosure attacks are very common in a lot of systems. This type of vulnerability, allows an attacker to access certain hidden pages through the web based management interface, which will disclose sensitive administrative information such as router name, software distribution or version numbers, patch levels, location of backup files or temporary files, administrative credentials etc. Example : “CVE-2013-3066 - NetGear WNDR4700 Unspecified Information Disclosure Vulnerability”

In the example of “CVE-2013-3066 - NetGear WNDR4700 Unspecified Information Disclosure Vulnerability”, the attackers can exploit this issue to obtain sensitive information that may lead to further attacks.

2.1.2 Domain Name System (DNS) Hijacking

Domain Name System (DNS) hijacking, is the attack of prevaricating the resolution of DNS queries. An attacker gains unauthorized access to the ADSL router web interface and altered or configured its DNS settings to point to a different set of DNS servers. This modifications forces all the network devices to point at a specially crafted, under the attacker's control, rogue DNS server. In this form of attack, a script (such as

JavaScript) or applets are used commonly on easily configured and deployed broadband routers and computers to create Denial-of-Service (DoS) attacks, steal data, infect system or change name resolution setting.

A typical sample on the risk of DNS hijacking attacks constitutes an attack which occurred on October 1st, 2012 in Brasil. Several Brazilian ISPs have fallen victims to a series of DNS hijacking attacks using 1 firmware vulnerability, 2 malicious scripts and 40 malicious DNS servers, which affected 6 hardware manufacturers, resulting in millions of Brazilian internet users falling victim to a sustained and silent mass attack on DSL modems.

2.1.3 Operating System (OS) Command injection

ADSL routers, are mostly embedded Linux devices. The main purpose of the operating system (os) command injection attack is to inject and execute arbitrary system commands specified by the attacker in the vulnerable application.

This fact can be exploited from adversaries to perform OS command injection attacks. As its name implies, the main purpose of an OS command injection attack is to inject and execute arbitrary system commands, specified by the attacker, through a vulnerable web page of the ADSL router. In particular, since most ADSL routers are Linux devices, the web application of the router is essentially a system shell.

Thus, an attacker may use the system shell to execute commands with the same privileges of the web application. The reason behind this attack is due to the lack of proper validation of the input data. Note that a web application, usually, takes input through forms (GET or POST) or other headers of HTTP requests (e.g., cookies, etc.). By replacing each possible input data with specific OS commands, the attacker can successfully perform this attack.

In the case of a vulnerable to os command injection form or field, because of lack of correct input data validation, in a web based management interface successful exploitation, allows an attacker to execute arbitrary system commands (e.x. like system shell) with the same privileges as the vulnerable application has (e.x root privileges). Example: “Cisco Linksys WRT54GL /apply.cgi wan_hostname Parameter Remote Command Execution”

In the example of “Cisco Linksys WRT54GL /apply.cgi wan_hostname Parameter Remote Command Execution” the Cisco Linksys “WRT54GL” suffers from a vulnerability that is triggered when input passed via the 'wan_hostname' parameter to the “/apply.cgi” script, that is not properly sanitized. This may allow a remote attacker to inject arbitrary os commands.

2.1.4 SQL injections

This well-known type of injection attack allows an attacker to inject code through the input data into to the application in order to execute arbitrary remote commands such us read sensitive information from the database, modify (e.x. Select, insert, delete, update) database's data, execute administration operations on the database. This attack exists because the web application does not validate the provided SQL query from the user before its processing. In embedded devices such as routers, the related database usually does not have any useful information from an attackers' point of view.

However, recently in [7] it was identified that a SQL injection vulnerability, he was able to to gain remote access to arbitrary files from the file systems of target device and to exploit a buffer overflow vulnerability in the DLNA (Digital Living Network Alliance) process. DLNA refers to set of specifications that define, among other things, mechanisms by which music and movie files may be served over a local network and played back by DLNA capable devices.

2.1.5 Denial of Service (DoS) Attacks

Denial of Service (DoS) Attack is basically a type of attack that a remote attacker aims to make a remote machine or network node, in our case the ADSL router, inaccessible by users or administrators. This means that the administrator, remotely, will not be able to access the web based administration interface and manage the router.

Apart from the issue of the lack of inaccessibility, the router is the device that connects Internet and the internal SoHo network so a Denial of Service (DoS) attack on the router can crash the device and cut internet access across the local network SoHo. Example : “TP-Link TL-WR740N Wireless Router Remote Denial Of Service Exploit”

In the example of “TP-Link TL-WR740N Wireless Router Remote Denial Of Service Exploit“ The attack occurs, when the malicious sending a sequence of three dots “...” to the router. This will crash the httpd service denying the legitimate users access to the admin control panel management interface. To bring back the http srv and the admin UI, a user must physically reboot the router.

2.1.5.1 Distributed Denial of Service (DdoS)

The distributed version of the DoS attack is the Distributed Denial of Service (DDoS) attack which is when many infected ADSL router devices (called as “zombies”) all together, launch the same attack against one or most victim hosts.

2.2 Client-side Attacks

Client-side attacks, attackers looking for ways to force an unsuspecting victim to process malicious code or data from a rogue server. In this way a client-side application can be provide information from a rogue server that results in some action taking place that is unintended or unexpected by the end user. It is also commonly hidden from the user.

This also shows the key to client-side attacks which to target those applications that interact with a server in some way. If this interaction is not present attacks of this type cannot take place. Client-side attacks targets vulnerabilities in client applications or triggered by a user action that interacts with a rogue server or process malicious data.

2.2.1 Session Hijacking Attacks

Session hijacking is an attack that taking control of a user session after successfully stealing or calculating an authentication session ID or session cookie (if the web-based authentication mechanism uses cookies as session identifier) and impersonating the legitimate user . The Session Hijacking vulnerability is caused due to an error in the session handling. Due to the wrongly use of the HTTP protocol (instead of HTTPS) in web-based authentication mechanism on several ADSL routers, all session data (session id, session cookie) transmitted in plain-text so could simply be sniffed (passively or through an ARP poison attack) from the local area network.

An attacker can easily capture all the traffic of a specific user and to compromise the session. If the ADSL router is vulnerable to Session Hijacking Attacks can be exploited by attacker to bypass the user authentication mechanisms and hijack to an administrative session. Except of stealing a user session, an internal *(either an external)* attacker can brute force, calculate or predict the session IDs or session cookies of a legitimate user's session while that session is still in progress.

Successful session hijacking attacks discloses sensitive information to authenticated users, since, they believe, it is the legitimate user who is accessing the page and allows execution of arbitrary commands with administrative privileges. Example : “2Wire 2700HGV-2 Broadband Router Session Hijacking Vulnerability”

In the example of 2Wire 2700HGV-2 Broadband Router Session Hijacking Vulnerability the web-based management interface of 2Wire Broadband router does not generate truly unique random session IDs for a logged-in administrator user. This allows attackers to brute-force guess a valid session ID to compromise the administrator session.

2.2.2 Cross Site Scripting (XSS) Attack

Cross-Site Scripting (XSS) attack is very commons type of injection attacks specifically on web based applications. In such attack malicious HTML or malicious javascript code is injected into trusted applications more specifically in the case of a vulnerable router's web interface the malicious injected code will execute in user's browser session.

These types of attacks rely on the inherent vulnerabilities present in web pages, namely the ability to run embedded code such as JavaScript. In this attack an attacker will inject code into a web page that will execute when a user visits, downloads and runs on their system. Programming code when run in this fashion can be used to steal personal information as well as run other code arbitrarily such as remote code exploits. The vulnerability stems from the fact that certain web pages are trusted more than others in the context of the web browser allowing code to run with higher privileges.

In such an attack an attacker exploiting the trust that a user has for a specific application or service. An attack type of XSS can have two states authenticated or unauthenticated. Example : “CVE-2013-3067 - Cisco Linksys WRT310N Router Unspecified Cross Site Scripting Vulnerability.”

In the example of CVE-2013-3067 - Cisco Linksys WRT310N Router Unspecified Cross Site Scripting Vulnerability the Cisco Linksys “WRT310N” Router is prone to an unspecified cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

This may help the attacker steal cookie-based authentication credentials and launch other attacks. This flaw exists because the application does not validate certain unspecified input before returning it to the user. This may allow an attacker to create a specially crafted request that would execute arbitrary script code in a user's browser within the trust relationship between their browser and the server.

2.2.2.1 Authenticated Cross Site Scripting (XSS) Attack

Authenticated Cross Site Scripting (XSS) Attack occurs when the vulnerability lies in a form or field of the router's web based management interface but, is accessible only for authenticated users so as it is reasonable the main target of the attack is the administrator or users that have access to the router's web based management interface.

2.2.2.2 Un-authenticated Cross Site Scripting (XSS) Attack

Unlike with the Authenticated Cross Site Scripting (XSS) attack the Un-authenticated Cross Site Scripting (XSS) attack occurs when the vulnerability lies in a form or field of the router's web based management interface and is accessible by all users on the SoHo network without any restriction or authentication therefore the target of attack is every single user on SoHo network.

2.2.3 Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is another very commons type of injection attacks specifically on web based applications. In such an attack the attacker exploiting the trust that a specific application or service has for the user. Particularly with Cross-Site Request Forgery (CSRF) attack an attacker forces an already authenticated user *(e.x. administration)* to execute unwanted actions (e.x. change administrator password, change DNS settings, restore router to default settings etc) on the router's web based management interface -in which is currently authenticated- as a result the attacker can compromise the device .

In conjunction with the Cross Site Scripting (XSS) attack and Domain Name System (DNS) hijacking cross-site Request Forgery can be extremely dangerous. Cross-site request forgeries (CSRF) attacks exploits the trust that a particular site (in our case the ADSL router's web interface) has with a user. Example: “D-Link DAP-1150 Cross Site Request Forgery Vulnerability”.

In the example of D-Link DAP-1150 Cross Site Request Forgery Vulnerability the device's web interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to e.g. change the administrator's password, reboot the device, or change the device configuration by tricking a logged in administrator into visiting a malicious web site.

3 Case Study : ZTE ZXV10 H108L ADSL Security Testing

The aim of this section is to investigate the security of a popular ADSL router named “ZTE ZXV10 H108L ADSL 2+ Wireless Router”, provided by the Telecommunication Company “WIND Hellas”. The router under investigation is an embedded device with MIPS CPU architecture. It includes a custom-made web interface for the device management, written in HTML and Java-script. During our security assessment, the ADSL router under testing had the latest available firmware (I.e., V1.0.01_WIND_A01).

After the security testing, we discovered two 0-day vulnerabilities in the web interface of the router. In particular, we discovered that the ADSL router is vulnerable to OS command injection and persistent XSS attacks. It is important to mention that these vulnerabilities were discovered by manual testing. We would like to note that all automated security checks, using well- known security tools failed to discover any vulnerability.

First, we discovered a stored XSS vulnerability (see figure 1) in a specific page of the web interface. For the successful exploitation of the XSS vulnerability, we added a specially crafted Javascript code in a field named “Host Name”. Since this XSS is stored, every time the user visits this specific vulnerable page, the malicious Java-script code will be executed.

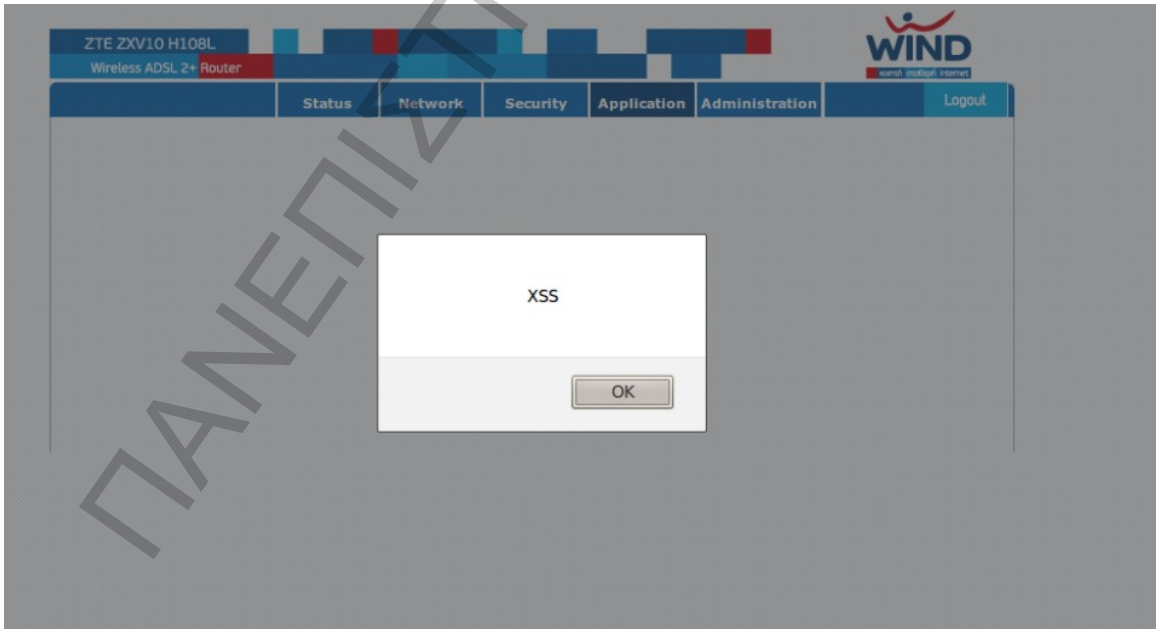

Figure 1 – The view of stored Cross-Site Scripting (XSS).

We used the following procedure for the discovery of the OS command injection vulnerability :

1. At first, we discovered that the ADSL router had the port 8083 open, which is used for remote access to the ADSL router through the Internet. This probably happens because the technical department of the specific ISP wants to have remote Internet access to the ADSL routers for troubleshooting purposes.

2. Next, we tried to establish a remote telnet connection using the default credentials for the admin account, but the telnet server of the ADSL router rejected the provided credentials. This means that the technical department of the ISP uses different credentials to establish a telnet connection with the ADSL routers.

3. Continuing our testing, we found a web page that performs diagnostic functionality to discover broken connections. We explored this page and discovered that this page, essentially, was executing the Ping command. After several trials and specially crafted input combinations to perform OS command injection, we succeeded to perform arbitrary command execution (see figure 2). At this point, we were able to execute all the command line tools provided with busybox.

Figure 2 – The view of Operating System (OS) command injection.

3.1.1 Methodology and results

By exploiting this vulnerability to perform command injection attacks, first we executed the command “uname” and we discovered that the specific ADSL router runs Linux OS, based on BusyBox v1.01 [10] (see figure 3).

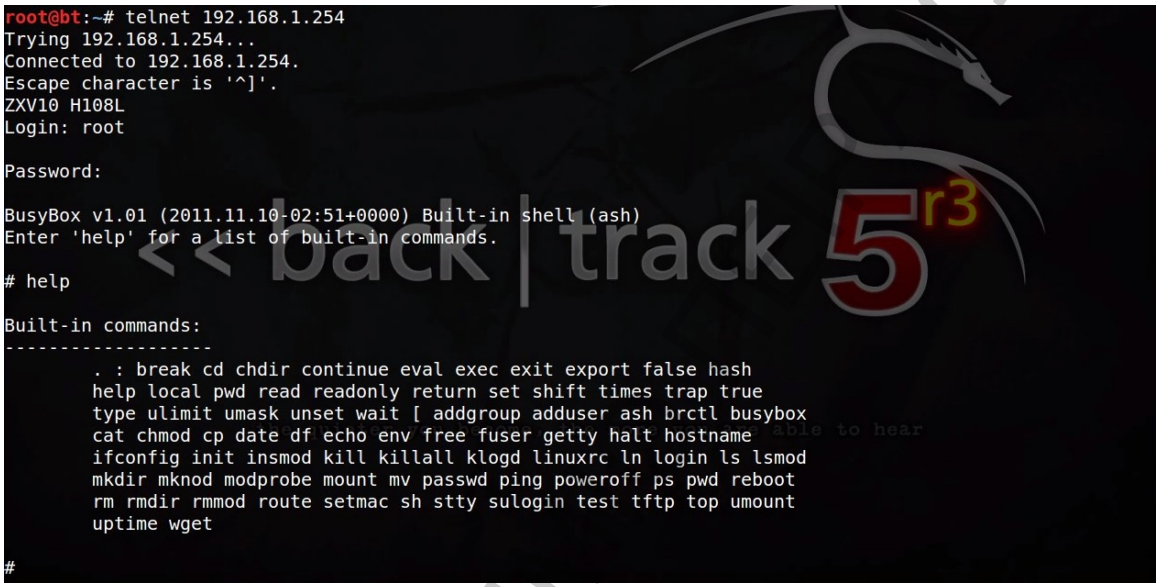

Figure 3 – The OS of ADSL router is based on BusyBox.

Next, we executed the command “vsftpd start” to activate the FTP service. After that, we successfully established an FTP connection using anonymous login credentials. After that, we downloaded for analysis several files of the busybox filesystem. In a file named “db_default_cfg.xml” we found in plaintext the secret password of the root account.

Then, we logged in using the discovered credentials of the root account (see figure 4) and we found that the ADSL router unlocked some hidden features, such as activating telnet services from LAN. We were also able to view hidden web pages that provided sensitive information about the Intranet network of the specific ISP, such as internal IP addresses.

The last testing that we made was to examine whether the same root password is used among other devices of the same model. For this reason, we have written and released a python script that automates the exploitation of the specific router [12].

We tested several other routers and in all cases we verified the assumption that all routers of the specific model share the same credential for the root account. This discovery is crucial, because it allows the attacker to perform generalized attacks as we analyze in section 4.

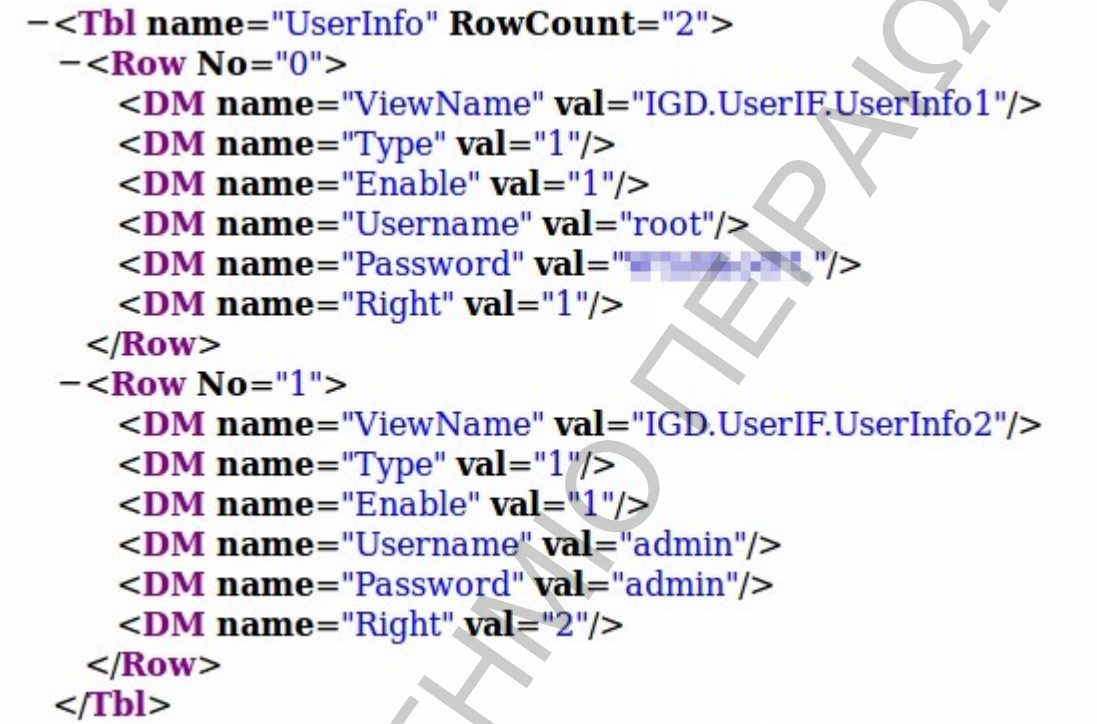

Figure 4 – The view of "/proc/cfg/db_default_cfg.xml"

4. Impact

Here we analyze the attacks that can be carried out from the discovered vulnerabilities. A malicious can exploit [12] the aforementioned vulnerabilities to perform a large-scale attack.

In particular, he/she can mount an automated attack by scanning and discovering IP addresses of the specific ISP. Next, he/she can gain unauthorized remote access to the specific routers simply by using the root account credentials, which is the same for the routers of the same model. At this point, the attacker has three different choices to complete his/her attack:

1. Perform a DNS hijacking attack. In particular, the attacker can replace the DNS settings of the ADSL router to point to a rogue DNS server, which is under the attacker's control. In this way, the attacker can achieve, for example, to direct the user of the ADSL router to a fake bank website instead of the legitimate bank website and steal his/her bank credentials. In other words, it can perform an effective phishing attack, which is undetectable.

2. Take advantage of the FTP connection to upload a sniffer that monitors the user's LAN traffic. A more devastating attack can be performed if the attacker uploads a malicious application that performs a DoS attack to a targeted server. In the last case, the attacker can combine several compromised and under his/her control ADSL routers to perform an orchestrated large-scale distributed DDoS attack.

3. Exploit the stored XSS to force the user to run a malicious java applet, which allows the attacker to have access to the user's personal computer, and through pivoting to exploit and gain access to the other devices or computers located in the local network of the compromised ADSL router.

5. Countermeasures

As mentioned previously vulnerable devices can generate quite unpleasant results, specially in generalized large-scale attacks. For this reason we will mention some countermeasures on the directly affected groups such as devices vendors / manufacturer and the end-users.

5.1 SoHo network devices vendors / manufacturers

SoHo network devices vendor / manufacturer should perform often security audits and vulnerability checks on devices that are in the process of production (pre-market) both at the application layer (firmware) and at the device layer (hardware). Vendors, should also update the firmware of devices that are available in the market in regular intervals.

On the official website, the vendor or manufacturer of the ADSL device should notify the consumers about the latest vulnerabilities that have been found in its products. Except the notification manufacturer should be provided the appropriate security patch which will solve the security problem is found. A proposed technique would be implemented by SoHo network devices manufacturers, could allow devices to automatically informed about the new vulnerabilities and updated by appropriate security patches.

5.1.1 Manufacturers countermeasures against server-side attacks

(i) Against Unauthorized Information Disclosure Attacks manufacturers must use strong authorization and strong encryption. The communication must be secured (HTTPS) with protocols that provide message confidentiality. Sensitive informations (ex: usernames, passwords etc) must be stored in encrypted databased and not in plain-text files (ex: xml files).

(ii) Against SQL injection Attacks or Operating System (OS) Command injections Attacks, manufacturers must validate and filter data coming from insecure sources, like user input. Some other techniques that could be used by manufacturers in combination, to protect the applications --that interact with users-- is “canonicalization” the technique to represent output data as data, and cannot possibly be represented as part of command, and White - Black listing technique in which creating lists of authorized and unauthorized input entries (by the user) which may have an application.

(iii) Against Denial of Service (DoS) Attacks manufacturers must use resource and bandwidth throttling techniques and must validate and filter data coming user input.

5.1.2 Manufacturers countermeasures against client-side attacks

(i) Against session hijacking attacks, manufacturers must use encrypted session negotiation is a fully-fledged protocol that supports multiple different end-to-end encryption functionalities. Use encrypted communication channels. Stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences.

(ii) Against Cross Site Scripting (XSS) or Cross-Site Request Forgery (CSRF) attacks, manufacturers must validate and filter data coming from insecure sources, like user input. Some other techniques that could be used by manufacturers in combination, to protect the applications --that interact with users-- is “canonicalization” the technique to represent output data as data, and cannot possibly be represented as part of command, and White - Black listing technique in which creating lists of authorized and unauthorized input entries (by the user) which may have an application.

5.2 SoHo network devices users

(i) After the first log-in on the administration panel, the default administrator's password must be replaced with a new, strong and secure, at least 12 characters in length, consisting of upper / lowercase alphanumeric and special characters.

(ii) Users should use the latest browser versions without making any deductions in safety and avoid visiting links that receive through e-mails or other social media (ex: facebook, twitter etc) and which starts with the ip address of the local network.

(iii) After logging out from the router, users must clear browser's cookies. Users should make sure that the Wireless LAN is protected using WPA2 encryption and is not left as an open WiFi network or protected with the outdated WPA or WEP standards.

(iv) The users should always upgrade ADSL router's firmware regularly, only from official manufacturer website.

6. Conclusions

This paper evaluated the security of ADSL routers by investigating vulnerabilities and analyzing possible attacks. As a case study we investigated the security of a popular ADSL router named “ZTE ZXV10 H108L ADSL 2+ Wireless Router”, provided by the Telecommunication Company “WIND Hellas”.

After the security testing, we discovered two 0-day vulnerabilities in the web interface of the router. In particular, we discovered that it is vulnerable to Operating ystem (OS) command injection and stored Cross-Site Scripting (XSS) attacks. A malicious may exploit these vulnerabilities to perform a large scale attack. Specifically, he/she can perform DNS hijacking and redirect the end users to fake web sites for phishing attacks; mount a Distributed Denial of Service (DDoS) attack; or even spread a malware.

We have disclosed the discovered vulnerabilities to the affected vendor of the router and the ISP that provides it. We promptly received a confirmation from the customers’ service department of the ISP that our request is being processed. However, at the time of writing this paper, we were not aware whether further actions have been taken from the ISP to patch the discovered vulnerabilities.

We believe that many Greek ISPs provide ADSL routers that are vulnerable to the same or similar attacks. To prove this, we have investigated another ADSL router, that is a “Baudtec” router, provided by the Greek ISP “OTE Conn-X” as we mentioned before, and we have found similar vulnerabilities, such XSS, CSRF Unauthorized Information Disclosure etc.

In general, the vulnerabilities are attributed to the poorly written software of these devices. It is evident that the ISPs in Greece are not aware of the security impacts and the harm that may cause such software vulnerabilities. ISP companies should perform strict security checks of their routers, before providing them to their customers. On the otherhand, end users should always patch and update the ADSL router with the latest available firmware for their device.

7. References

[1] State of Broadband in Greece Second Quorter 2012, Hellenic Telecommunications & Post Commisions, http://www.eett.gr/opencms/export/sites/default/EETT/Electronic_Communications/TelecommunicationServicePurchase/broadbandServices/Broadband_stats_2012-Q2.pdf , 2012

[2] Brazilian hackers use DNS poisoning to infect users with banking Trojan, http://www.infoworld.com/d/security/brazilian-hackers-use-dns-poisoning-infect-users-banking-trojan-178421

[3] Exploits Database, Offensive Security, http://www.exploit-db.com/

[4] Packet Storm, http://packetstormsecurity.com/

[5] RouterPwn framework, http://routerpwn.com/

[6] Router Exploitation, Felix "FX" Lindner, http://www.recurity-labs.com/content/pub/FX_Router_Exploitation.pdf,2010

[7] SQL Injection to MIPS Overflows: Rooting SOHO Routers, Zachary Cutlip, http://media.blackhat.com/bh-us-12/Briefings/Cutlip/BH_US_12_Cutlip_SQL_Exploitation_WP.pdf,2012

[8] Cross-site Scripting (XSS), https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

[9] OS Command Injection, https://www.owasp.org/index.php/OS_Command_Injection

[10] BusyBox, http://www.busybox.net/

[11] Client-Side Attacks and Defense, Oriyano Sean-Philip, Robert Shimonski

[12] ZTExploit, https://github.com/stasinopoulos/ZTExploit

[13] Hristo Bojinov, Elie Bursztein, Eric Lovett, Dan Boneh, "Embedded Management Interfaces: Emerging Massive Insecurity ", BlackHat 2009, USA.

[14] DirBuster: a multi threaded java application designed to brute force directories, OWASP