The weakest link on the network: exploiting ADSL routers to perform cyber-attacks!

Anastasios Stasinopoulos, Christoforos Ntantogian, Christos Xenakis
Department of Digital Systems, University of Piraeus
Piraeus, Greece
{stasinopoulos, dadoyan, xenakis}@unipi.gr

Synopsis: ADSL routers are an integral part of today's home and small office networks. Typically, these devices will have been 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 cybercriminals to quickly and easily gain control over a network. This research aims at investigating 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 System (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 poisoning 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.

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 login process using a browser.

Motivation

Recently, there has been a lot of discussion regarding the security of SoHo ADSL routers. For example, it was discovered that several Brazilian ISPs have fallen victims of a series of DNS hijacking attacks, via unauthorized access to the ADSL router's web interface [2]. The attacks had compromised about 4.5 million ADSL routers. Once compromised, users were redirected to specially crafted phishing domains that mainly targeted users' online banking credentials. Although many individual researchers have investigated the security of the ADSL routers ([3], [4], [5], [6], [7]), to the best of our knowledge there is no prior work on the security of ADSL routers that the Greek ISP's provide to their customers. This research aims at investigating the security of a popular ADSL router named "ZTE ZXV10 H108L ADSL 2+ Wireless Router", provided by the Telecommunication Company "WIND Hellas". The specific ADSL router had the latest available firmware.

Methodology and results

The router under investigation is an embedded device with MIPS architecture. It includes a custom-made software for the device management, written in HTML and Javascript. 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 Operating System (OS) command injection [8] and stored Cross-Site Scripting (XSS) [9] attacks. It is important to mention that these vulnerabilities were discovered by manual testing. On the other hand, all automated security checks that we performed, using security tools, failed to discover any vulnerability.

Regarding the OS command injection vulnerability, first we discovered that the ADSL router allows telnet access, only, through the Internet (WAN), and not over the local network (LAN). This happens, probably, because the technical department of the specific ISP wants to have remote Internet access to the ADSL routers for troubleshooting purposes. However, we were not able to establish a telnet connection using the default and publicly known credentials for the "admin" account. This means that the ISP uses different credentials to login. From the diagnosed functionality of the ADSL router's web interface, we managed, after several trials and various combinations, to perform OS command injection. By exploiting this vulnerability, we, first, found that the specific ADSL router runs Linux OS based on BusyBox [10]. Next, we activated the FTP service. After that, we established an FTP connection by using the anonymous login credentials. Then, we downloaded and analyzed several files (i.e., "/etc/shadow", "/etc/db_default_cfg.xml", "/proc/cfg/db_default_cfg.xml"). In one file we found the existence of a hidden account, named as "root" along with its secret password, in plaintext. By using the root account credentials, we found that the ADSL router unlocked some hidden features (such as allowing telnet services from LAN) and we were able to view information about the intranet network of the specific ISP. Finally, it is important to mention that we have verified that the same credentials are also used in other devices of the same model.

Except of the OS command injection, we discovered a stored XSS vulnerability 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 javascript code will be executed.

Impact

A malicious can exploit 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, simply, by using the root account credentials. At this point, the attacker has three different choices to complete his/her attack:

(i) Replace the entries in the DNS record (i.e., DNS poisoning) with a rogue DNS server, under the attacker's control, to direct the user to a fake bank website and steal bank credentials (i.e., phishing).

(ii) Exploit the stored XSS in order to force the end-user to run a malicious application to perform a DDoS attack combined with other compromised ADSL routers.

(iii) Exploit the stored XSS to force the user to run a malicious java-applet that allows the attacker to have access to the user's personal computer and through pivoting to other devices or computers located in the same network with the compromised ADSL router.

Conclusions

In this research, we focused on the vulnerabilities that we identified in the specific ADSL router and we highlighted their security consequences. 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", and we have found similar vulnerabilities, such XSS and CSRF. 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 other

hand, end users should always patch and update the ADSL router with the latest available firmware for their device.

References

[1] State of Broadband in Greece Second Quarter 2012, Hellenic Telecommunications & Post Commisions, available at 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, available at https://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems, 2012

[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, available at http://www.recurity-labs.com/content/pub/FX_Router_Exploitation.pdf, 2010

[7] SQL Injection to MIPS Overflows: Rooting SOHO Routers, Zachary Cutlip, available at 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/