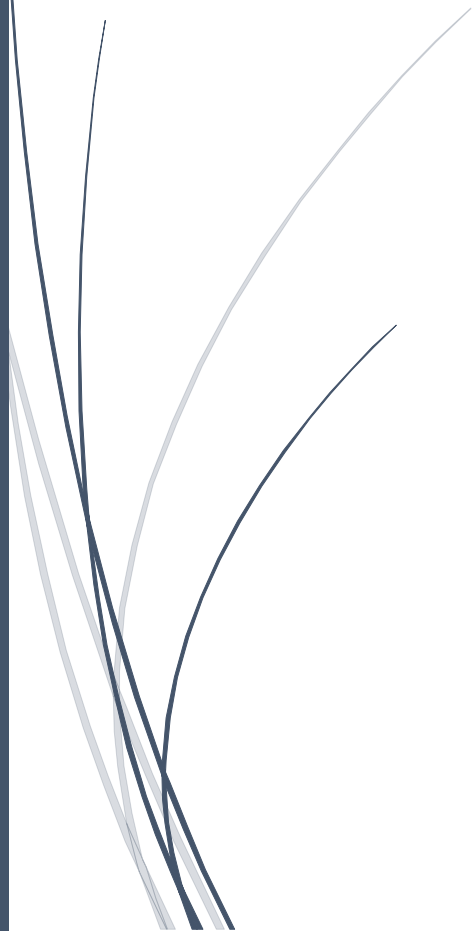
UNIVERSITEIT TWENTE.

1-11-2015

Individual Assignment – Economics of Security

Diego Sainz



University of Twente
MASTER COMPUTER SECURITY

Contents

Abstract

A lot of cyber-attacks aim routers or SCADA devices every day. Most of these security incidents are caused by agents which act moved by economic incentives. Several countermeasures can be taken to reduce the number of attacks and to mitigate the impact of these attacks for the end user and other actors. Patch management constitutes an important mean to avoid the vulnerabilities of routers and SCADA firm wares. This paper proposes a method to measure to what extent patch management is improving every year in order to protect routers and SCADA devices against the most frequent cyber-attacks, and if it is correct to analyze routers and SCADA devices simultaneously. To do so, two famous brands of routers and two famous brands of SCADA devices have been chosen and their different corrected vulnerabilities have been analyzed.

I. Introduction

Every day, cyber-attacks against governments and commercial computer networks number in the millions. For example, according to U.S. Cyber Command, pentagon systems are probed 250 000 times per hour. Similar attacks are becoming more prevalent on other kinds of information-based smart networks as well, such as those that operate buildings and utility systems. If the objective is to steal intellectual property or halt operations, the tools and the strategies used for unauthorized network access are increasingly sophisticated.

It is known that ADSL routers are an integral part of today's home and office networks. Typically, these devices 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.

Besides, there is increasing concern regarding cybersecurity across industries where companies are steadily integrating field devices into enterprise-wide information systems. This occurs in discrete manufacturing and process industrial environments, a wide range of general and specific purpose commercial buildings, and utility networks. Traditionally, electrical systems were controlled through serial devices connected to computers via dedicated transceivers with proprietary protocols. In contrast, today’s control systems are increasingly connected to larger enterprise networks, which can expose these systems to similar vulnerabilities that are typically found in computer systems.

This paper focuses on two vulnerable types of devices: routers and SCADA devices. These devices are the targets of several types of attack, such as distributed denial-of-service (DDoS), Cross-site scripting (XSS) or Overflow for instance. Several countermeasures can be taken in

order to avoid the risk, accept the risk and its potential consequences, transfer the risk to another sector or entity or mitigate the risk by preventative or proactive action. Among these countermeasures and risk mitigation strategies, patch management is a famous mean to reduce the number of vulnerabilities of a device. Just as a reminder, a patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. Patch management software offers companies the ability to abide by industry best practices while also complying with any applicable regulatory requirements for the securing of IT systems against possible malware or unauthorized intrusions. However, every countermeasure needs an incentive from the problem owner and to have a good ratio benefits/costs. Nowadays, patch management is a never-ending cycle, therefore it is important to determine in what extent this countermeasure contributes to the security of routers and SCADA devices. To do so, two famous companies of routers (D-Link and Netgear) and two famous companies of SCADA devices (Siemens and Rockwell Automation) have been chosen and their different corrected vulnerabilities analyzed.

II. Literature Review

First, an interesting paper is "Recommended Practice for Patch Management of Control Systems" [1] by DHS National Cyber Security Division Control Systems Security Program. In it, the patch management processes of traditional information technology (IT) data networks and industrial control systems (ICSs) are separated. Indeed, it is stated that IT patching typically requires relatively frequent downtime to deploy critical patches, but any sudden or unexpected downtime of ICSs can have serious operational consequences. So, there are more requirements for patch validation prior to implementation in ICS networks. Then, the paper describes vulnerability analysis, in relation to patch management, which is the process of determining when and if a patch should be applied to the ICS. A qualitative method is used: the vulnerability footprint which consists of four subjective, primary elements (Impact, Exposure, Deployment, and Simplicity) that create a graphical representation of the vulnerability footprint in the shape of a diamond. An example of vulnerability footprint is given on Figure 1. Finally, this paper has identified resources that provide additional information on cyber threats, vulnerabilities, self-assessment tools and recommended practices that may be used to incorporate ICS patch management processes into existing IT security plans. Unfortunately, this tool is only qualitative.

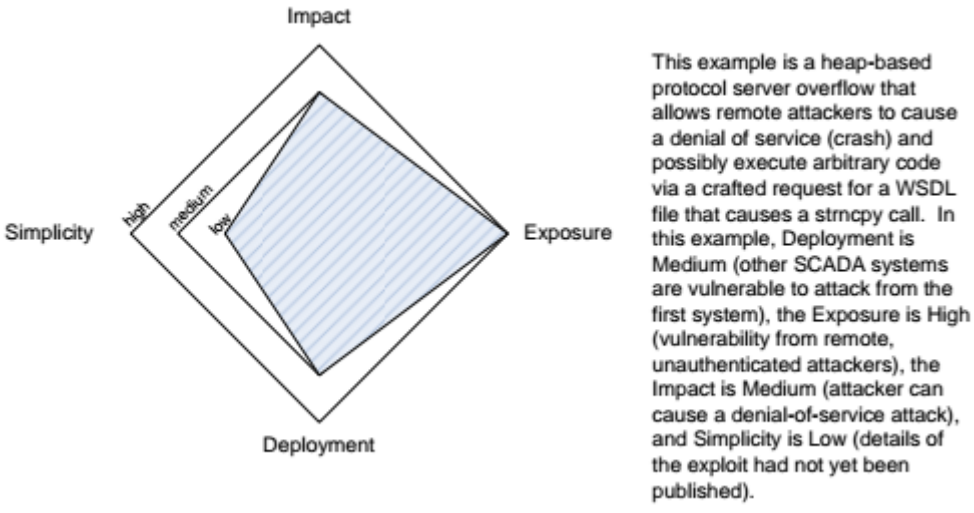


Figure 1: Example of Vulnerability footprint

Then, "A Taxonomy of Cyber Attacks on SCADA System" [2] by Bonnie Zhu, Anthony Joseph and Shankar Sastry highlights the differences between SCADA systems and standard IT systems, then presents a set of security property goals. Furthermore, it focuses on systematically identifying and classifying likely cyber-attacks including cyber-induced cyber-physical attacks on SCADA systems. The paper states that SCADA systems generally have little protection from the escalating cyber threats and that factors like the continuous availability demand, time-criticality, constrained computation resources on edge devices, large physical base, wide interface between digital and analog signals, social acceptance including cost effectiveness and user reluctance to change, legacy issues and so on make SCADA system a peculiar security engineering task. Some vulnerabilities are described such as "No Privilege Separation in Embedded Operating System", "Buffer Overflow" and "SQL Injection". The paper concludes by mentioning a pressing need for robust SCADA-specific intrusion detection systems (IDS) and resilient control. This paper did not take Patch management as a good solution to remove the vulnerabilities of SCADA systems.

Another interesting paper on the subject is "Rewriting the rules of patch management" [3] by IBM. The author says that Patch management has always been an uphill climb because of the massive complexity involved, and despite the risks, some organizations are reluctant to patch because of the time and labor required, plus the potential of disrupting business operations. IBM gives a solution named "Endpoint Manager" in six steps: Research, Assesses, Remediate, Confirm, Enforce, and Report. Their results have included faster deployment, better compliance, reduced IT costs and shorter management cycles. IBM concludes by saying that this solution can be the difference between a successful patch management strategy and one that leaves the organization at risk.

Next, "Patch management: Fixing vulnerabilities before they are exploited" [4] by GFI is an interesting paper on the matter. It shows the importance of Patch management, and, using 2010 data from the US National Vulnerability Database, gives the top 10 applications targeted for vulnerabilities. Three important points of Patch management are given: instability, compatibility and driver clashes. These points are the reasons why an organization might need

or choose to revoke a software update that has been pushed out by a vendor and installed. The author concludes the paper by saying that a robust patch management solution that combines swift roll-back of problem patches with a single view of what patches are installed on machines across the organization, is a critical component of both software management and IT security strategies. Finally, such a solution will ensure that applications are not placed at unnecessary risk, while ensuring that a policy of encouraging end-users to accept and install critical updates at the first possible opportunity can be maintained.

Another great paper which covers the subject is "Patch Management: Best Practices" [5] by Chris Roberge. In it, the problem stated is that many organizations today do not have an effective maintenance plan in place to protect their assets and the solution is an effective patch management procedure. Mr. Roberge talks about the challenges of Patch management saying that today, patching has become a process that affects all platforms and applications as more and more security vulnerabilities are being discovered and exploited by more and more sophisticated hackers. The Figure 2 illustrates the number of vulnerabilities reported by the CIAC (Computer Incident Advisories Capabilities) over the last few years and demonstrates the steady increase in the total number of vulnerabilities exposed annually.

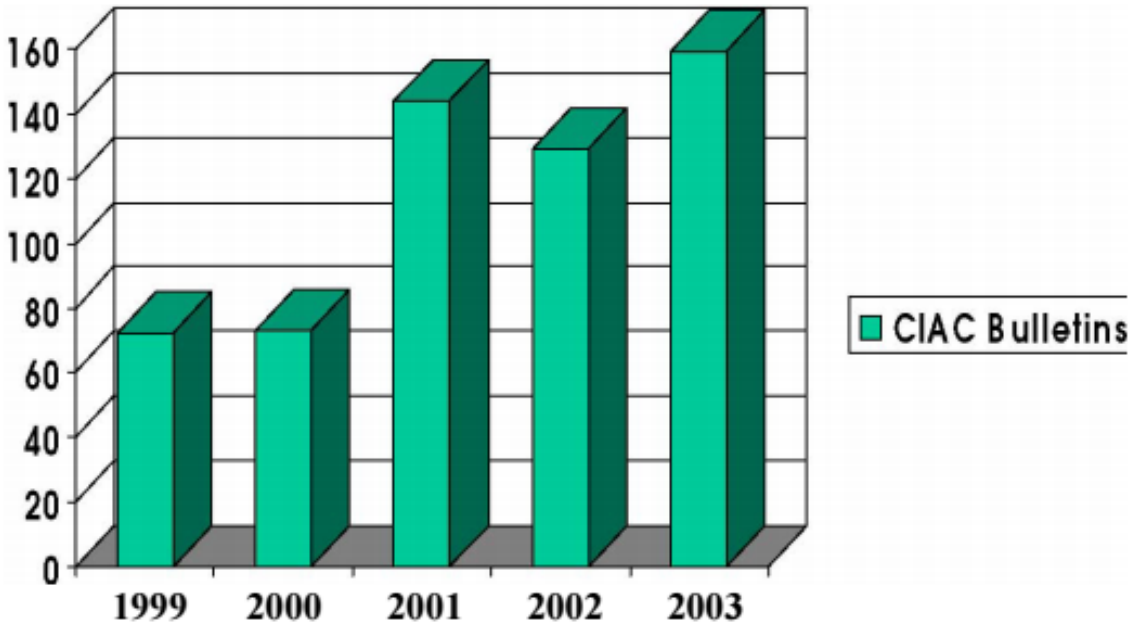


Figure 2: Number of vulnerabilities reported by the CIAC from 1999 to 2003

The paper concludes by saying that Patch management requires the regular rediscovery of systems that may potentially be affected, scanning of those systems for vulnerabilities, downloading patches and patch definition databases, and deploying patches to systems that need them.

Finally, all the papers highlight the importance of Patch management, but they also show its weaknesses and some notable differences between patching routers and patching SCADA devices.

III. Research question, Objective and Hypothesis

1) Research question

What is the evolution of Patch management on SCADA devices and domestic routers?

2) Sub questions

In what extent Patch management on routers has improved over the years?
In what extent Patch management on SCADA devices has improved over the years?
Are these evolutions similar for routers and SCADA devices in spite of their differences?

3) Hypothesis

As we can guess from the patch-oriented papers of the literature review, Patch management is improving every year and reduces the number of attacks on SCADA devices and routers. SCADA devices suffer from much more attacks than routers, due to their little protection [2] but Patch management is an effective countermeasure to take in order to mitigate the cyber risks. Besides, we can assume that Patch management is improving more slowly for SCADA devices.

IV. Methodology (Research Design)

The research method consists in analyzing the most numerous vulnerabilities on routers and SCADA systems, taking 2 top companies specialized on routers and 2 top companies specialized on SCADA devices. In that way, the dataset from the group assignment can be used, and completed to answer the research question. Then, the metrics are listed and the statistical technique is explained.

1) Routers

Routers are networking devices that forward data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data packets are typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node. The most common types of routers are home and small office routers that simply pass data, such as web pages, email, and videos between computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through an ISP.

Routers are one of the favorite targets for cyber-attackers because they lie outside of several security protections. It is known that attackers target specific routers and firmware versions and can access to the routers via weak or default credentials. When the router is compromised, they overwrite the firmware with modified and malicious versions designed to run on the specific hardware. These attackers probably bought these routers new or purchased used ones off eBay in order to reverse engineer the firmware and create malicious versions. Modifying firmware for the attacker’s needs or to add new features is a typical practice and has been used to great success on home routers and access points. This is the same practice used on a larger scale in order to facilitate cyber-attacks. The new firmware operates like the original but has some added features that allow the attackers to snoop on the traffic passing through the device. In order to protect themselves, organizations have to tightly control access to their routers, use strong secured passwords, and monitor them closely for configuration changes that can indicate compromise.

In order to classify the key vulnerabilities of routers, 2 top routers companies have been chosen: D-Link and Netgear. D-Link Corporation, founded in March 1986, is a Taiwanese multinational networking equipment manufacturing corporation headquartered in Taipei, Taiwan. Netgear, Inc. is an American global networking company that delivers products to consumers, businesses and service providers. The Figure 3 and 4 show the discovered vulnerabilities of D-Link and Netgear routers in History from Table 1 and Table 2 of CVE details (Appendix).

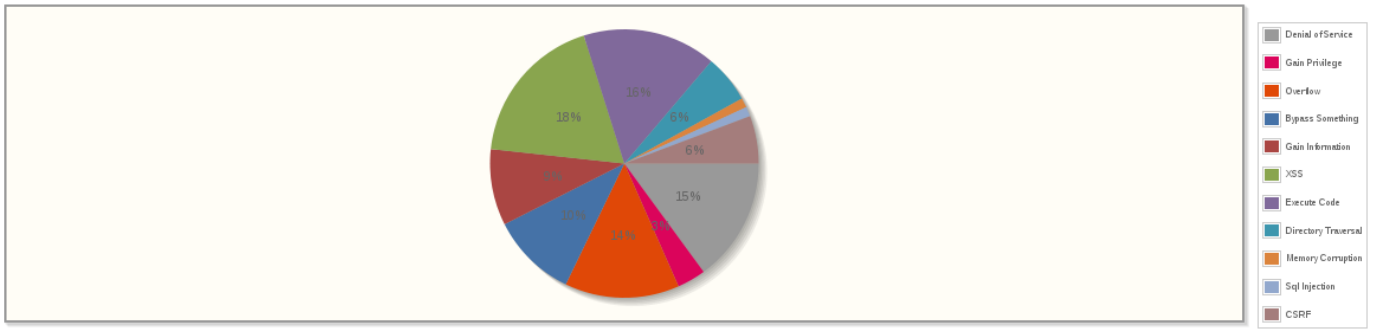


Figure 3: D-Link vulnerabilities

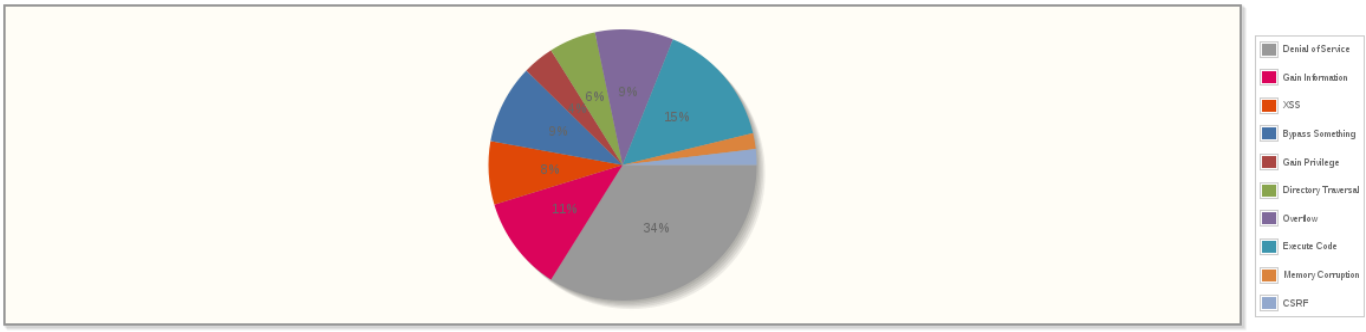


Figure 4: Netgear vulnerabilities

These graphs show that the most numerous vulnerabilities for routers are DoS, XSS, code executions and overflows. To be clear, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. The cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications, allowing attackers to inject client-side script into web pages viewed by other users. The code

execution is used to describe an attacker's ability to execute any commands of the attacker's choice on a target machine or in a target process. Finally, an overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

2) SCADA devices

SCADA (Supervisory Control and Data Acquisition) devices are devices running a system that operates with coded signals over communication channels to provide control of remote equipment, using in general one communication channel per remote station. The control system can be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions. SCADA is a type of Industrial Control System (ICS). Industrial control systems are computer-based systems monitoring and controlling industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large-scale processes that can include multiple sites, and large distances.

The security of SCADA and real-time systems represents a significant challenge in today's world. High profile cyber security threats are a recent phenomenon (for instance, the Stuxnet or Night Dragon attacks) and the systems running critical industrial processes are typically a generation older. Consequently, there are many legacy systems that may be vulnerable to cyber-attacks because cyber security was simply not a consideration at the time of initial design and installation. The security of even recently deployed systems may also be an issue, and often there are media reports of instances where systems are connected to the internet with inadequate protection, or the manufacturers of the equipment have used hardcoded usernames and passwords, thereby offering cyber intruders the ability to manipulate the system settings.

In order to classify the key vulnerabilities of SCADA devices, 2 top SCADA companies have been chosen: Siemens and Rockwell Automation. Siemens AG is a German multinational conglomerate company headquartered in Berlin and Munich. It is the largest engineering company in Europe, having for main divisions: Industry, Energy, Healthcare, and Infrastructure

& Cities. Rockwell Automation, Inc. is an American provider of industrial automation and information solutions. Its brands include Allen-Bradley and Rockwell Software. Headquartered in Milwaukee, Wisconsin, Rockwell Automation employs over 22,000 people and serves customers in more than 80 countries worldwide. The Figure 5 and 6 show the discovered vulnerabilities of Siemens and Rockwell Automation SCADA devices in History from Table 3 and Table 4 of CVE details (Appendix).

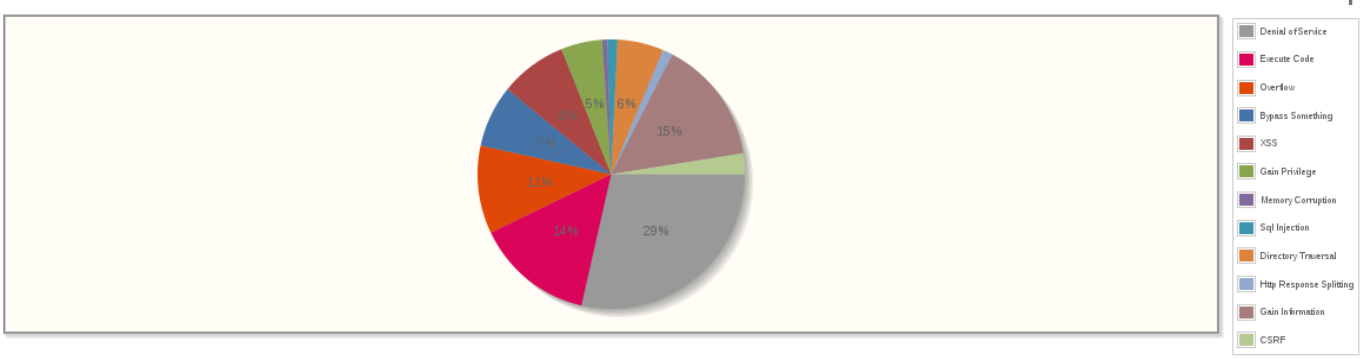


Figure 5: Siemens vulnerabilities

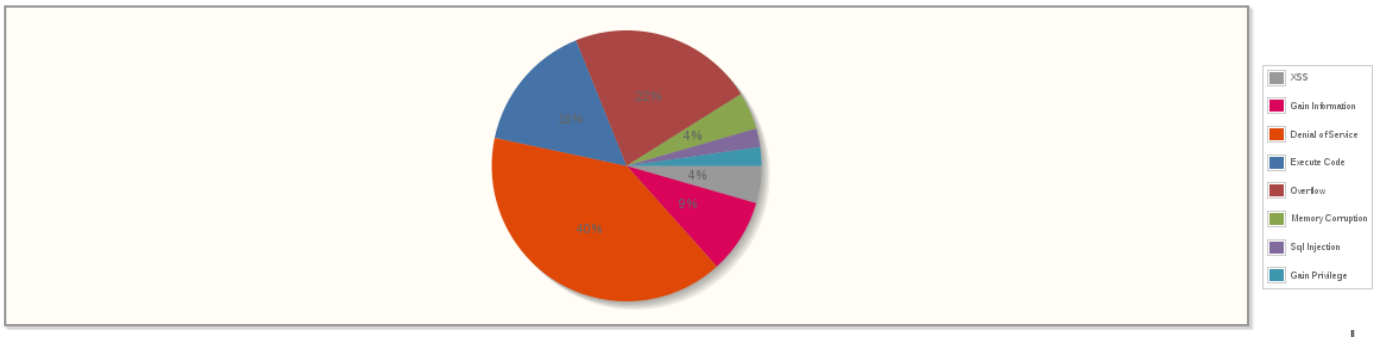


Figure 6: Rockwell Automation vulnerabilities

These graphs highlight that the most numerous vulnerabilities for SCADA devices are DoS (most important vulnerability), code executions and overflows. The fact that DoS is the most important vulnerability of SCADA devices was predictable because these devices being used in the industry, a DoS can have a huge impact on the company, stopping its activities. XSS is not a main vulnerability of SCADA devices, contrary to routers.

3) Metrics

Considering the group 3 dataset and the research question, different types of metrics can be put in place, depending on the organization. Besides, these metrics are both applicable to routers and SCADA devices:

- Percentage of each known vulnerability per company
- Number of vulnerabilities per year
- Number of vulnerabilities per company
- Number of days before patching each vulnerability (and the type of the vulnerability)
- Average number of days before patching a vulnerability per year

4) Statistical analysis

First of all, the evolution of the number of vulnerabilities of routers and SCADA devices will be qualitatively compared, using Tables 1 – 2 – 3 – 4 (Appendix), in order to see if the routers and the SCADA devices follow approximately the same trend or not.

Then, a linear regression "y = a + b*x" between the average number of days to patch a vulnerability and the years of successful correction will be made for each company. After that, the slopes will be compared and a qualitative comparison of the evolution of the patching time will be made.

The figure 7 show an extract of the dataset used for the assignment, for example the D-Link routers vulnerabilities patched in 2015. In it, the number of days before patching has been calculated by using the Excel function DATEDIF and then the average number of days before patching per year has been calculated by using the Excel function AVERAGE.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Nb of days
1	CVE-2015-2052	119		Exec Code Overflow	2/23/2015	2/24/2015	1
2	CVE-2015-2051	77		Exec Code	2/23/2015	2/24/2015	1
3	CVE-2015-2050			Exec Code	2/23/2015	3/18/2015	23
4	CVE-2015-2049			Exec Code	2/23/2015	3/18/2015	23
5	CVE-2015-2048	352		CSRF	2/23/2015	2/24/2015	1
6	CVE-2015-1028	79	3	XSS	1/21/2015	1/26/2015	5
						Average :	9

Figure 7: D-Link 2015 patched vulnerabilities from CVE details dataset

V. Results

First, the Figure 8 shows the evolution of the number of vulnerabilities of routers and SCADA devices:

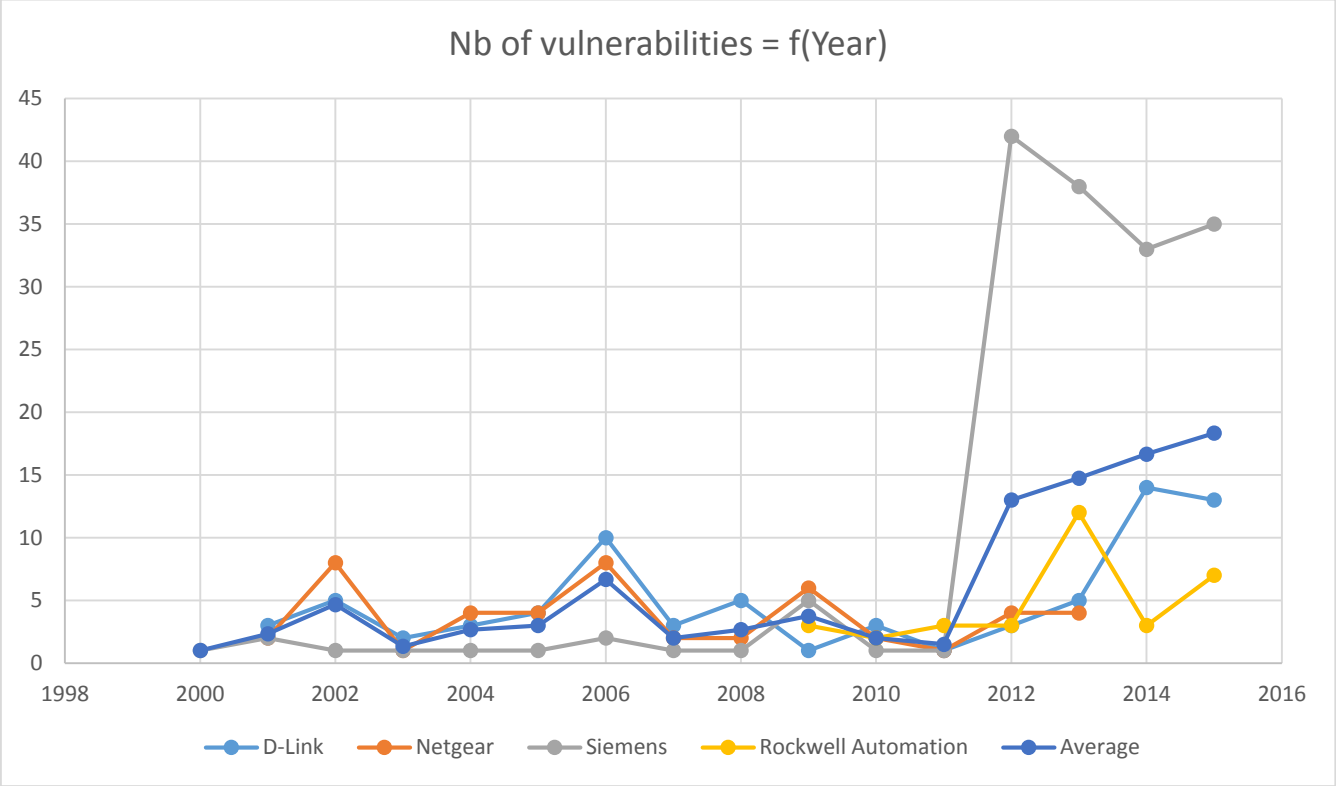


Figure 8: Evolution of the number of vulnerabilities of routers and SCADA devices

Several inferences can be made. Globally, the number of vulnerabilities for each brand is increasing, probably because the number of different routers and SCADA devices is increasing. Moreover, the evolution of the technology causes discoveries of new vulnerabilities and the cyber-attackers become smarter and smarter. Next, 2006 is a bad year for routers and SCADA devices, with more vulnerabilities for all the brands than 2005 or 2007 (except Rockwell Automation). For Siemens, 2012 is a black year, but except this gap, the trend is very similar for routers and SCADA systems, which does not match with the hypothesis.

Secondly, the Figures 9-10-11-12 are the results of a linear regression y = a + b*x where y = average number of days before patching a discovered vulnerability and x = year. The patching time can be highly variable because it can depend on the complexity of the vulnerability, given in the dataset but not integrated in the model. The Figure 13 is the summarizing table of the slopes found in the Figures 9 to 12.

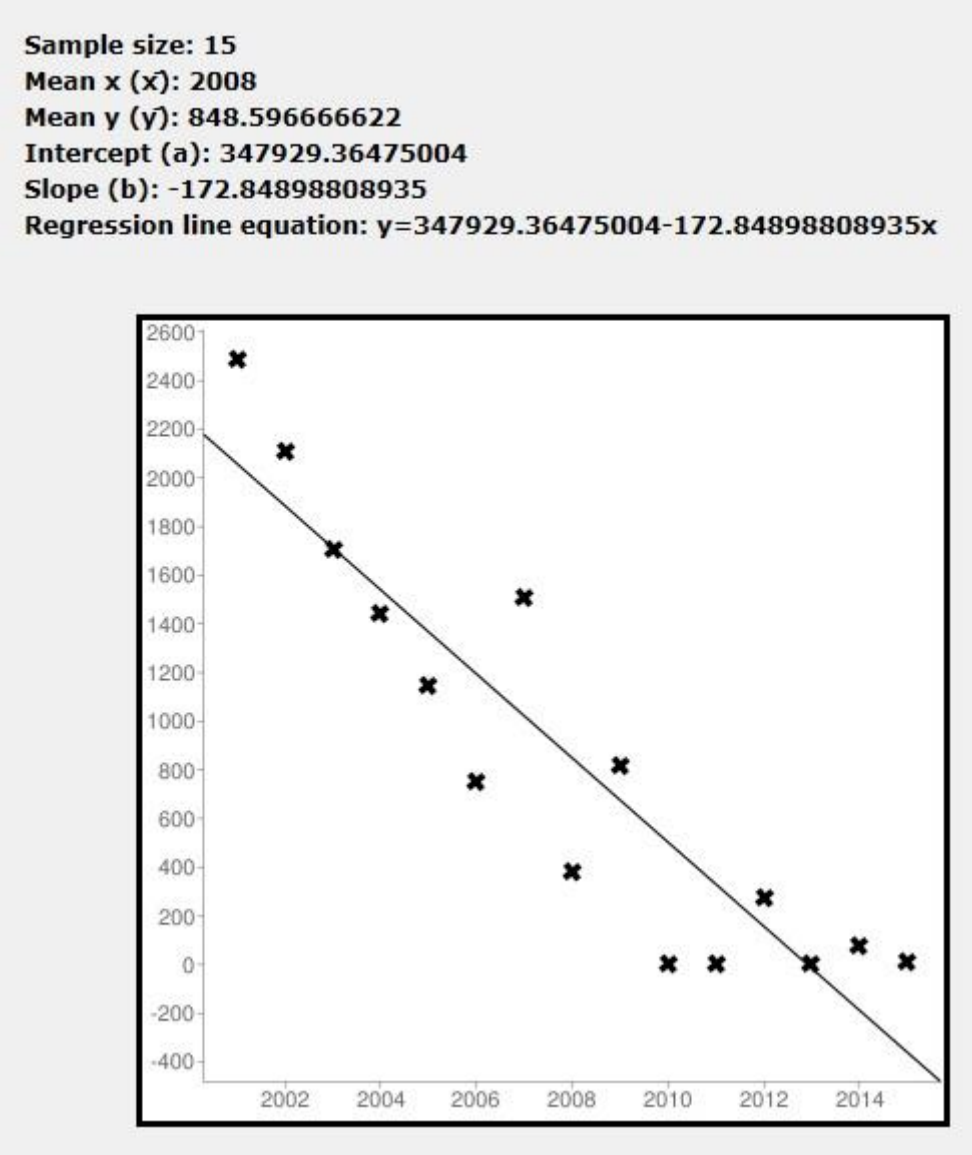


Figure 9: Linear regression of (D-Link) Nb of days before patching = f(Year)

Sample size: 14
Mean x (x̄): 2007.5
Mean y (ȳ): 835.98630952379
Intercept (a): 400527.43470694
Slope (b): -199.09910256409
Regression line equation: y=400527.43470694-199.09910256409x

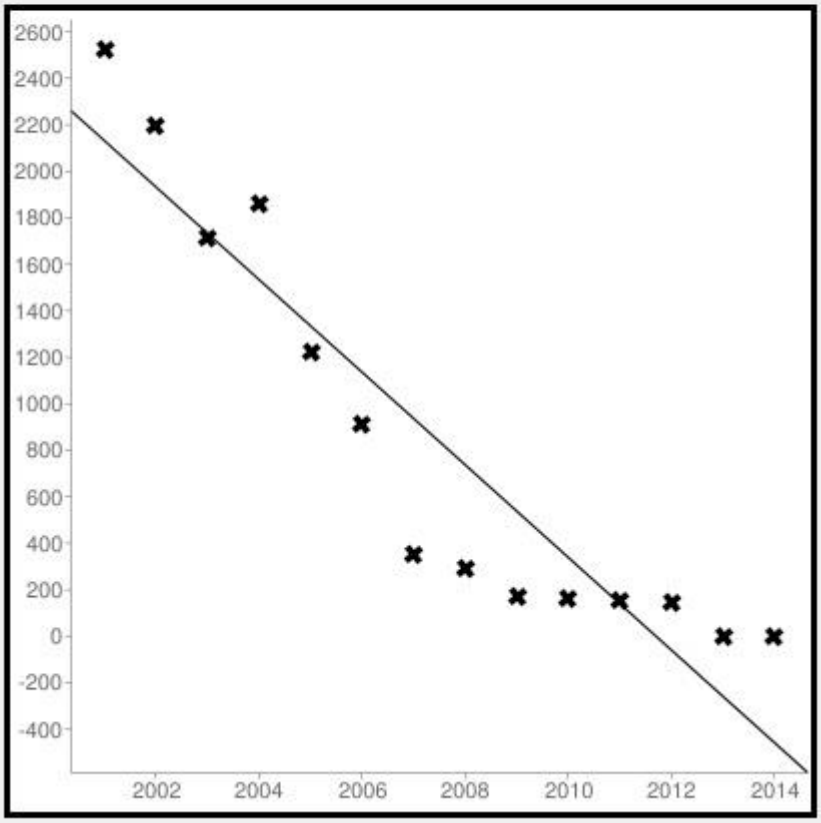


Figure 10: Linear regression of (Netgear) Nb of days before patching = f(Year)

Sample size: 17
Mean x (x̄): 2007
Mean y (ȳ): 1118.7079206239
Intercept (a): 437706.95984786
Slope (b): -217.53276129907
Regression line equation: y=437706.95984786-217.53276129907x

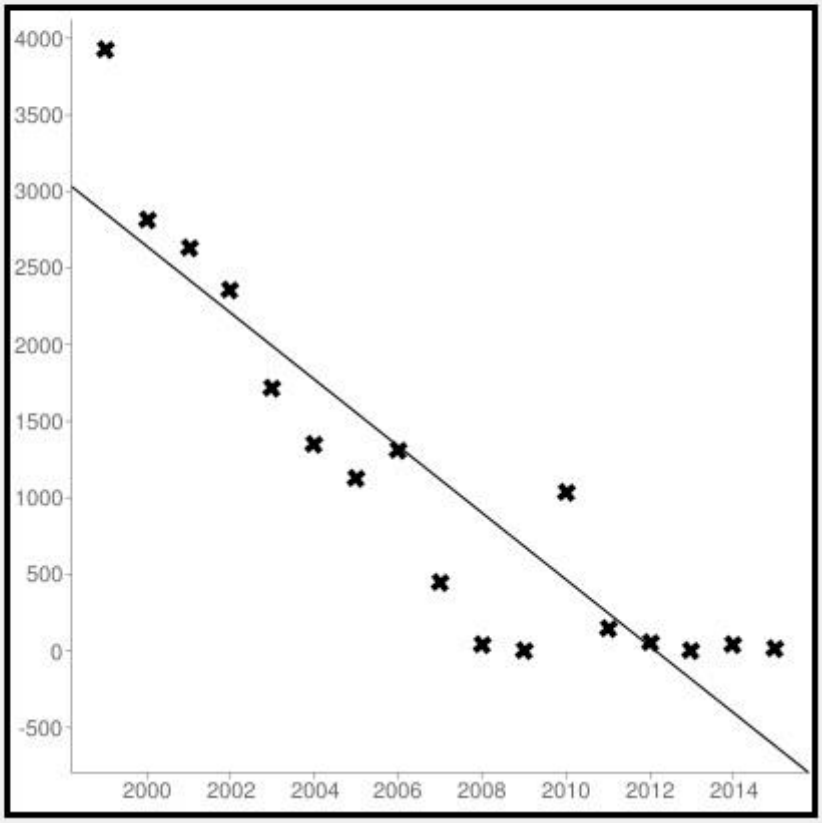


Figure 11: Linear regression of (Siemens) Nb of days before patching = f(Year)

Sample size: 7
Mean x (x̄): 2012
Mean y (ȳ): 43.802380957143
Intercept (a): 42271.850000964
Slope (b): -20.988095238572
Regression line equation: y=42271.850000964-20.988095238572x

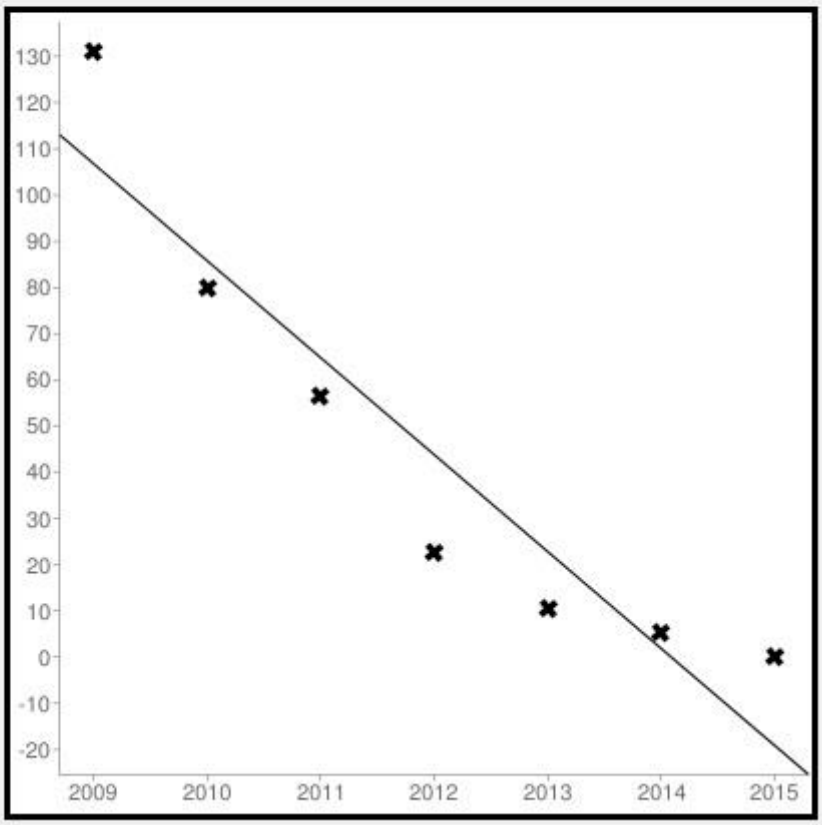


Figure 12: Linear regression of (Rockwell) Nb of days before patching = f(Year)

	D-Link	Netgear	Siemens	Rockwell Automation
Slope	-173	-199	-217	-21

Figure 13: Summarizing slopes table relative to the linear regressions

Several deductions can be made from these figures. First of all, the four functions do not seem so similar, so we cannot propose a generic function for routers and SCADA devices. However, the slopes b are very similar according to the Figure 13, around -195, except for

Rockwell Automation but we can suppose that this difference is due to the lack of data in the dataset (for example, Siemens sample size = 17 and Rockwell Automation sample size = 7). Then, we can highlight the fact that the average patching time over the years is very similar for the two brands of routers: 836 and 849 days. Concerning the SCADA devices, the average patching time is very different to routers' and between the two companies as well.

Finally, the Figure 14 summarize the patching time evolution of routers and SCADA devices. The positive point is the reducing patching time over the years, for both routers and SCADA devices. Then, except 2 points for D-Link and 1 for Siemens, the trend is very similar, in harmony with the conclusions about the slopes. The trend is represented by the average curve.

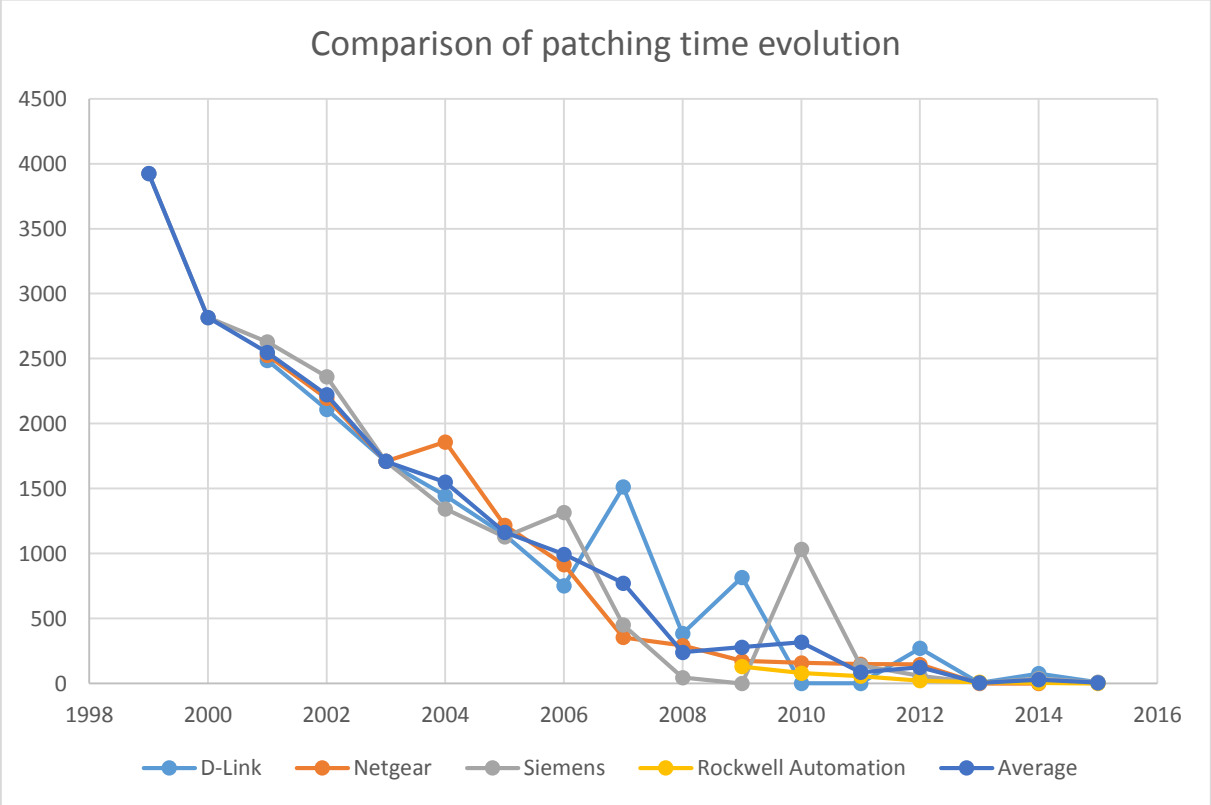


Figure 14: Evolution of the number of vulnerabilities of routers and SCADA devices

VI. Limitations

The first limitation of this research method is the lack of data in the dataset. Indeed, getting the number of attacks on routers and SCADA devices for example could bring more interesting results about patch management. Then, taking only two companies for routers and SCADA devices is not the best way to find a good trend, for example Rockwell Automation was not the best choice in this study.

Next, the monetary cost of purchasing automated patch management software has not been treated because it is as varied as the many patch management products on the market. There are freeware versions of patch management products, there are standalone products for those with a budget but also on a budget, and there is patch management software that is integrated within an all-encompassing monitoring and management software suite. The main problem here is the fact that there is no one right answer for which type of patch management software is the best fit for a specific situation. Each method of patch management software licensing represents a different price point and feature set that will help guide organizations to the best product within their budget.

VII. Conclusions

To conclude and answer the research question, the evolution of Patch management is greatly improving for routers and for SCADA systems. Indeed, the number of days needed for patching a vulnerability was around 2500 days in the years 2000 and is now only few days. Therefore, we can assume that the companies D-Link, Netgear, Siemens and Rockwell Automation followed the Patch management best practices and solutions [1] [3] [4] [5].

Aside from a few accidents, the trend of Patch management is relatively similar for routers and SCADA devices, therefore they can be gathered for studying this countermeasure. Taking into account the difficulty of patching SCADA devices [2], this result is surprising, however it can be considered very positive. The linear regressions emphasized a similar slope for routers and SCADA devices patching time over the years and an average time very similar for routers.

References

[1] “Recommended Practice for Patch Management of Control Systems” - DHS National Cyber Security Division Control Systems Security Program

[2] “A Taxonomy of Cyber Attacks on SCADA System” - Bonnie Zhu, Anthony Joseph and Shankar Sastry

[3] “Rewriting the rules of patch management” – IBM

[4] “Patch management: Fixing vulnerabilities before they are exploited” - GFI

[5] “Patch Management: Best Practices” - Chris Roberge

Appendix

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2001	3	1										1			
2002	5	2		1						1	2				
2003	2											1			
2004	3	1					1								
2005	4	1								2	1	1			
2006	10	2	2	2			2	2			1				
2007	3	2		1	1										
2008	5	1	1	2			2			1					1
2009	1		1	1											
2010	3	1					2								1
2011	1										1				
2012	3	1	1	1						1	1				1
2013	5		2	1						1	1				3
2014	14	1	2	2		1	5	3		2			2		2
2015	13		5	1			4			1	1		3		3
Total	75	13	14	12	1	1	16	5		9	8	3	5		11
% Of All		**17.3**	**18.7**	**16**	1.3	1.3	**21.3**	6.7	0	12	10.7	4	6.7	0	

Table 1: D-Link routers vulnerabilities over the years according to CVE details

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2001	2	2									1				
2002	8	3					1			1	2	1			
2003	1							1							
2004	4	1								1					
2005	4	1		1			1			1					
2006	8	3	3	3	1						1	1			
2007	2						1								
2008	2	2	2												
2009	6	4	1					2		1					4
2011	2									1					
2012	1														
2013	4	1	1								1		1		1
2014	4	1	1	1			1				1				1
Total	48	18	8	5	1		4	3		5	6	2	1		6
% Of All		**37.5**	**16.7**	**10.4**	2.1	0	**8.3**	6.3	0	10.4	12.5	4.2	2.1	0	

Table 2: Netgear routers vulnerabilities over the years according to CVE details

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2000	1	1	1	1											
2001	2	1													
2002	1	1													
2003	1	1		1											
2004	1														
2005	1														
2006	2	1								1					
2007	1	1					1								
2008	1	1													
2009	5	3								1					4
2010	1											1			
2011	1	1	1	1	1										
2012	42	11	8	8		1	5	4	1	1	2	1	1		5
2013	38	5	8	5		1	4	2	1	4	7	2	1		
2014	33	13	3				2	2			3	3	1		
2015	35	6	2	1			1	1		5	12	1	1		
Total	166	46	23	17	1	2	13	9	2	12	24	8	4		9
% Of All		**27.7**	**13.9**	**10.2**	0.6	1.2	7.8	5.4	1.2	7.2	14.5	4.8	2.4	0	

Table 3: Siemens SCADA devices vulnerabilities over the years according to CVE details

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	3						1				1				
2010	2	1													
2011	3	2	2	2	1										
2012	3	3		1											
2013	12	9	2	5							1				
2014	3	2	1								1				
2015	7	1	2	2	1	1	1				1	1			
Total	33	18	7	10	2	1	2				4	1			
% Of All		**54.5**	**21.2**	**30.3**	6.1	3	6.1	0	0	0	12.1	3	0	0	

Table 4: Rockwell Automation SCADA devices vulnerabilities over the years according to CVE details