Vulnerability Statistics for 2011

POSITIVE RESEARCH

POSITIVE / TECHNOLOGIES®

Table of contents

1 Introduction

SecurityLab.ru issued an annual report that provides statistics on vulnerabilities published in 2011. The researchers were focused on SCADA systems, content management systems (CMS), Adobe applications, browsers, and Windows-based operating systems. All these applications and systems were frequently penetrated last year. This review covers some serious incidents triggered by allegedly insignificant vulnerabilities, and gives the corresponding statistics.

Vulnerabilities as a Way to Block Production or Stop Nuclear Program

In 2011 specialists confirmed that Cyber Cold War had broken out. Today hackers are targeting industrial plants and military facilities. Last fall was welcomed with a Trojan famous as Duqu. It penetrates a Windows-operated computer by exploiting the CVE-2011-3402 vulnerability. Then it can make its way to the enterprise's SCADA system, steal the information about the IT infrastructure and establish control over the industrial facilities. Some experts noted that components of the main Duqu module resembled those of the Stuxnet warm, which had incapacitated several Iranian uranium enrichment plants in 2010.

Forged SSL Certificates – Revenge for Iran?

In the spring and summer of 2011, hackers from Tehran compromised servers of Comodo and DigiNotar certification authorities. The DigiNotar operation turned out to be more "successful": some of the stolen certificates belonged to the CIA, Mossad, and MI6. Beside the needs of international cyber intelligence, the stolen digital passports were used to conduct man-in-the-middle attacks (MitM). The hackers redirected "client's" Internet traffic to their proxy, where the victim browser received the forged certificate and returned non-encrypted information. Those operations put at risk users of many services that use SSL certificates such as Internet banking, email etc.

Digital Signature and US Military Secrets

Having hacked servers of RSA Security in March 2011, unknown hackers jeopardized security of RSA SecurID digital signatures. Over 40 million employees used those tokens to access restricted networks. The attack started with an email that offered the staff members of the RSA headquarters to open a spoofed Excel file with an intriguing name *Recruitment Plan 2011.xls*. If opened, the malicious worksheet triggered the installation of Poison Ivy by exploiting the CVE-2011-0609 vulnerability in Adobe Flash Player. The stolen data contained information on the newest solutions for two-factor authentication. Later, the hackers tried to use the tokens to break into servers of the world's biggest military industrial system, Lockheed Martin.

Non-Compliance with PCI DSS: What Are the Threats?

In May, 2011, the police captured a group of Rumanian hackers who had cracked transaction processing systems in vending machines and during the next three years had been intercepted data from clients' payment cards. Their main victim was Subway. According to *The Wire*, the Subway LAN was penetrated via wireless networks and the vending machines were not compliant with Payment Card Industry Data Security Standards (PCI DSS). Moreover, the specialists who provided remote technical support services for the equipment made fatal errors. Not only had they failed to install updates for PCAnywhere, a remote administration application, but they had used the simplest password-login combination (*administrator*, *computer*) for more than 200 systems.

2 The Status of Vulnerabilities (Available Patches)

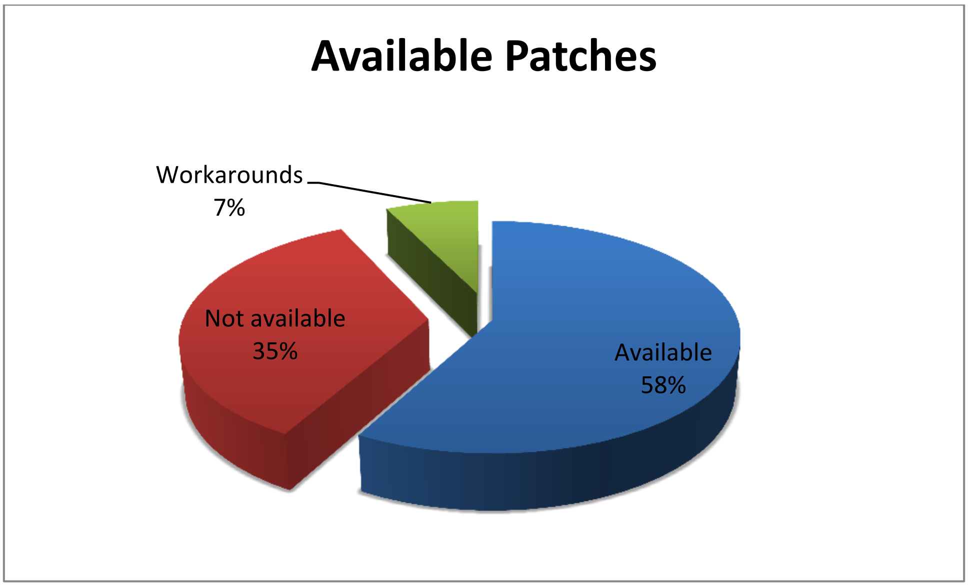

Figure 1. Vulnerability Status (Available Patches)

The total number of vulnerabilities described in 2011 is 4733. By January 1 vendors were able to fix only 58% of vulnerabilities and publish workarounds for 7%. This means that more than a third of the vulnerabilities remained exploitable for cyber criminals.

3 Distribution of Vulnerabilities Based on Type of Action

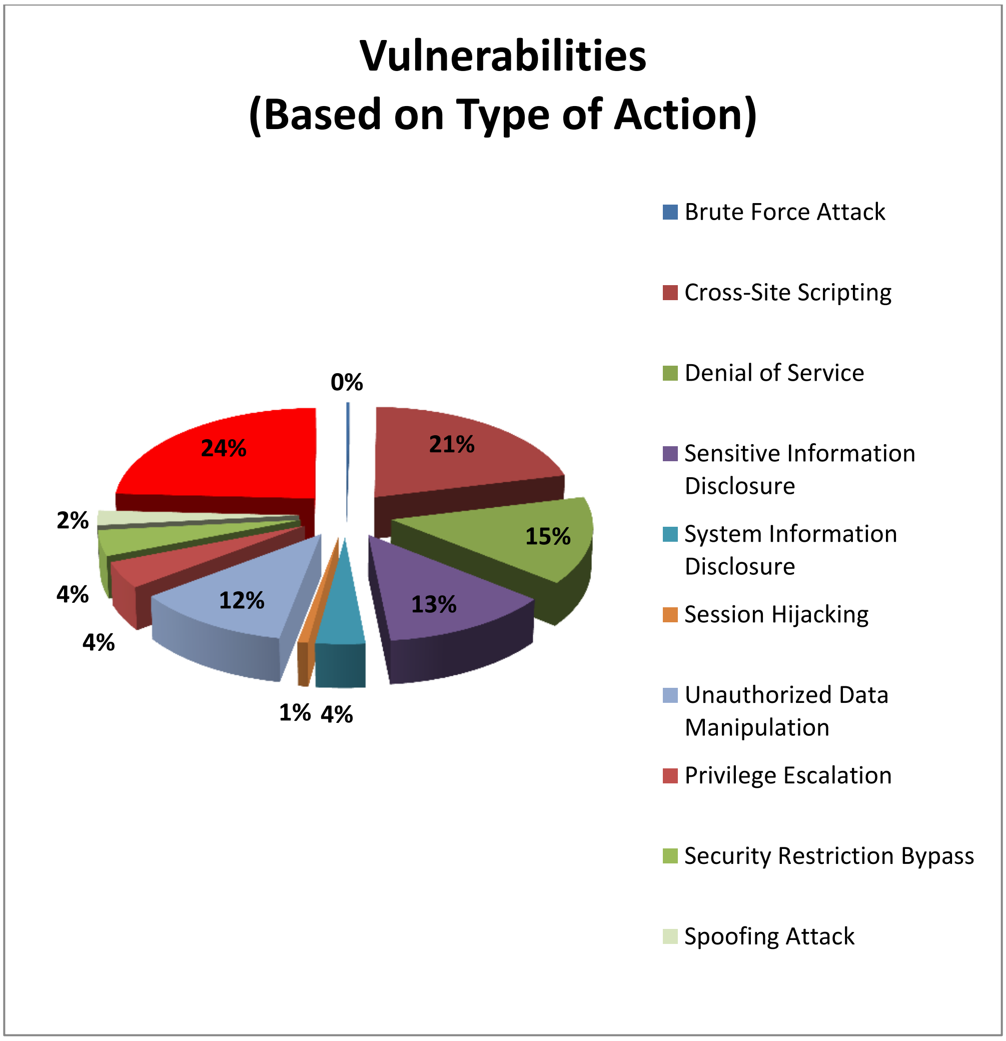

Figure 2. Distribution of Vulnerabilities Based on Type of Action

Almost a quarter of vulnerabilities (24,2%) allowed hackers to compromise a system by executing arbitrary code on the victim`s computer, 21% led to Cross-Site Scripting, about 15% could trigger denial of service. 13% of the detected flaws could be used for sensitive information disclosure. Finally, 12% allowed unauthorized data manipulation.

4 Distribution of Vulnerabilities Based on Exploitation Vector

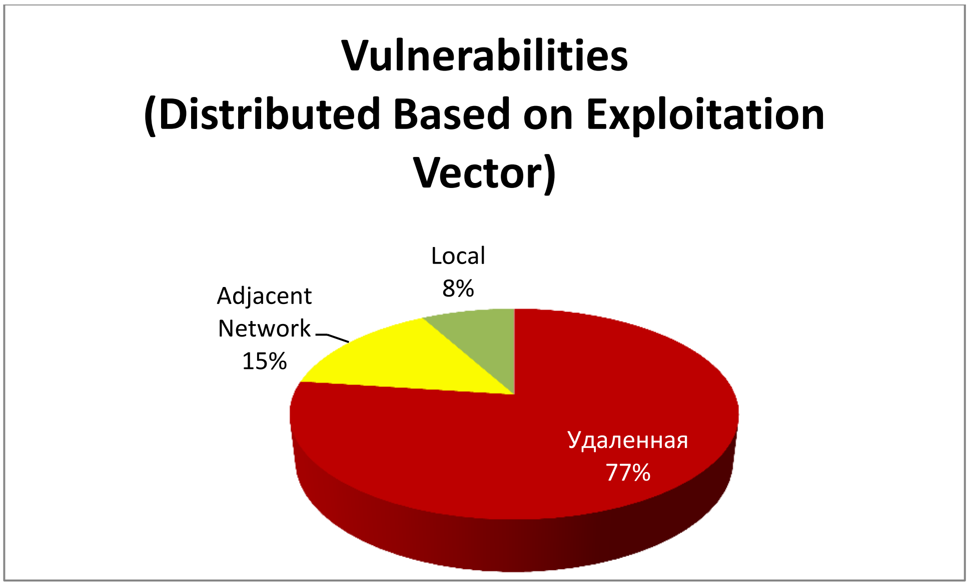

Figure 3. Distribution of Vulnerabilities Based on Exploitation Vector

77% of all the vulnerabilities detected in 2011 could be exploited remotely, 15% - over the local network and 8% required local access.

5 Vulnerabilities Sorted By the Type of Software

Let’s look at vulnerabilities in the types of software solutions provided below.

1. Server Software

Table 1. Vulnerabilities in Server Software

Type of Software\Severity	High	Medium	Low
SCADA systems	1	24	12
DNS servers	2	7	—
Web servers	2	9	13
Application Servers	3	5	22

Vulnerabilities in SCADA systems were in the limelight: 17 security bulletins described 37 vulnerabilities. Such attention to software component of SCADA is not unreasonable: last two years were favorable for viruses that targeted industrial automation applications.

2. Client Software

Table 2. Vulnerabilities in Client Software

Type of Software\Severity	Critical	High	Medium	Low
Browsers	4	425	77	88
Office Applications	3	127	7	16
Multimedia Applications	—	247	13	10
ActiveX components	3	83	5	11

3. Browsers

Over 594 vulnerabilities were detected in the most popular browsers (the summary table is provided below).

Note: Errors of the Denial of Service type were not considered in the report.

Table 3. Browser Vulnerabilities

Browser\ Severity Level	Vulnerability	Critical	High	Medium	Low
Apple Safari	169	—	140	13	16
Google Chrome	278	1	197	42	38
Mozilla Firefox	89	—	65	12	12
Internet Explorer	39	3	20	3	13
Opera	19	—	3	7	9

In 2011, Google Chrome fixed more vulnerabilities than other browsers, with Apple Safari following it and Mozilla Firefox being the third.

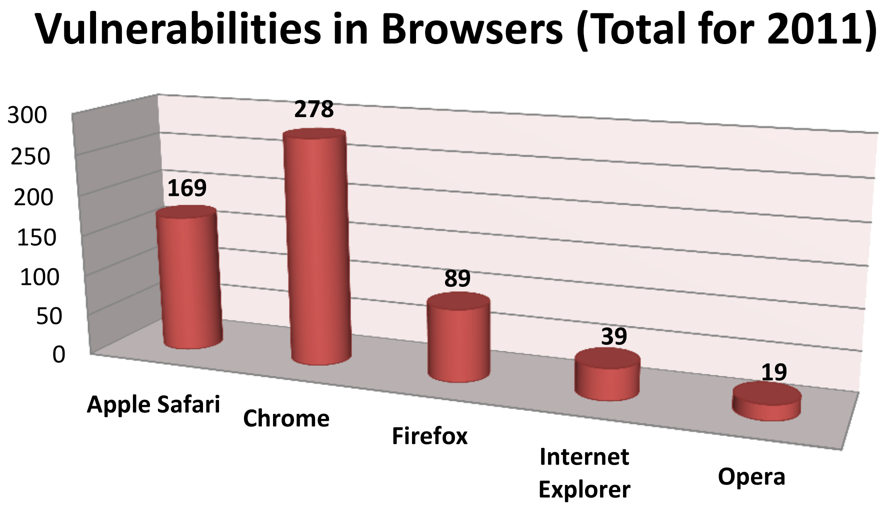

Figure 4. Browser Vulnerabilities

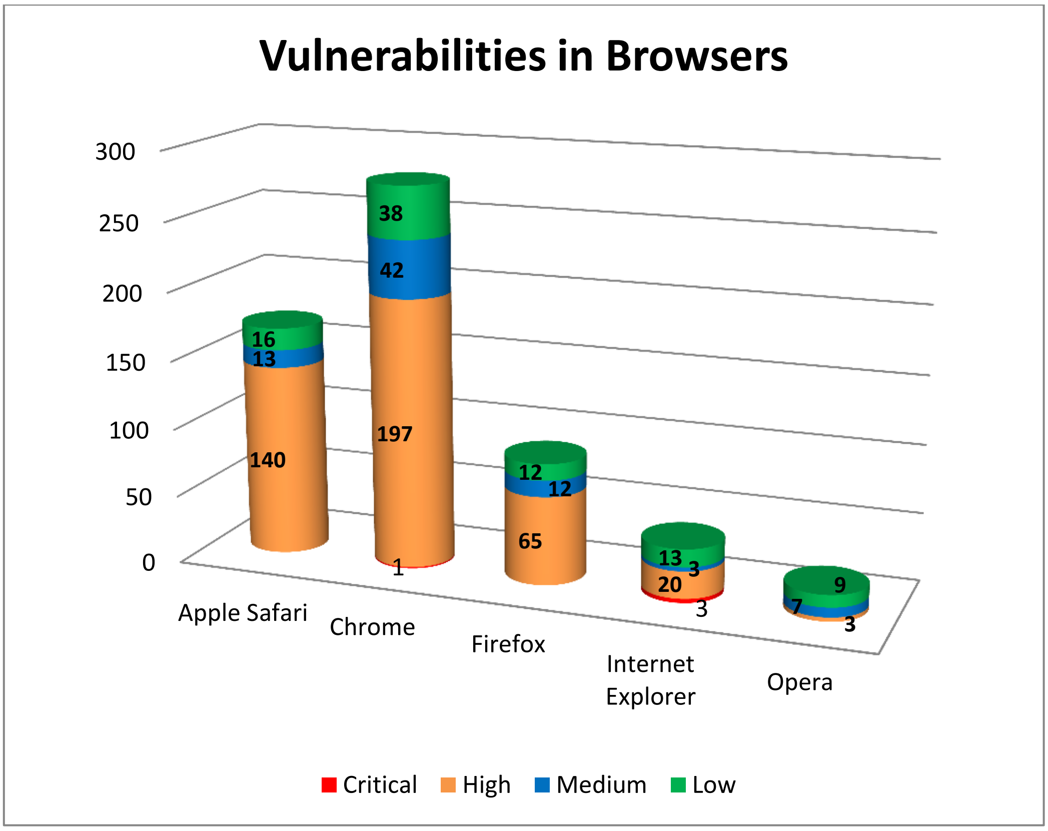

Figure 5. Distribution of Browser Vulnerabilities Based on Their Severity Level

Judging by the number of vulnerabilities, the most secure browser of 2011 is Opera. All other applications of this type proved to contain numerous severe vulnerabilities that could lead to system compromise. Among the vulnerabilities, there were 4 critical ones, which had been used in various successful attacks on a number of companies. Three of them were detected in Internet Explorer and one, in Chrome 11.x.

Table 4 provides total statistics for vulnerabilities detected in various browser versions.

Table 4. Vulnerabilities in Various Versions of Popular Browsers

Browser\Severity Level	Critical	High	Medium	Low
Apple Safari 5.x	—	140	13	16
Google Chrome 8.x	—	16	4	2
Google Chrome 9.x	—	43	8	3
Google Chrome 10.x	—	23	3	4
Google Chrome 11.x	—	12	5	2
Google Chrome 12.x	1	26	9	1
Google Chrome 13.x	—	40	9	3
Google Chrome 14.x	—	17	2	8
Google Chrome 15.x	—	20	1	16
Internet Explorer 6	3	16	2	11

Internet Explorer 7	3	15	2	12
Internet Explorer 8	2	17	3	11
Internet Explorer 9	1	14	2	10
Mozilla Firefox 3.5.x	—	18	3	3
Mozilla Firefox 3.6.x	—	34	6	4
Mozilla Firefox 4.0.x	—	11	—	3
Mozilla Firefox 5.0.x	—	7	1	1
Mozilla Firefox 6.0.x	—	7	1	1
Mozilla Firefox 7.0.x	—	5	1	2
Mozilla Firefox 8.0.x	—	4	1	2
Opera 10.x	—	1	1	4
Opera 11.x	—	3	7	8
Opera Mobile for Android 11.x	—	—	—	1

4. Popular Media Players

Table 5. Vulnerabilities in Popular Multimedia Players

Product\Leverity Level	High	Medium	Low
Apple iTunes 10.x	133	1	3
Apple QuickTime	27	—	2
RealPlayer 14.x	22	—	—
VLC Media Player	14	1	—
Winamp	17	—	—
Windows Media Player	2	—	—

In 2011, the chart of most vulnerable popular media players was leaded by Apple iTunes (133 vulnerabilities). The widely used VLC Media Player is in the middle of the list (15 vulnerabilities), while Windows Media Player contained only two vulnerabilities, which is almost 70 times less than in Apple iTunes.

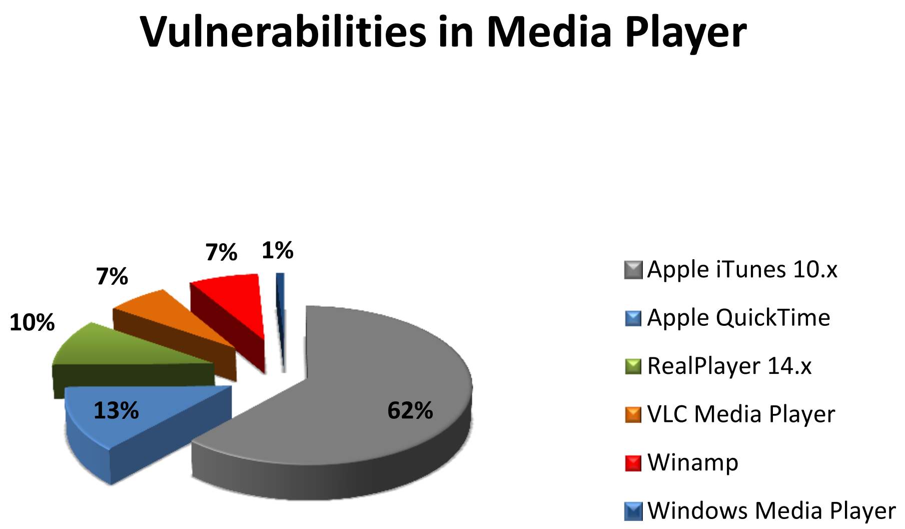

Figure 6. Vulnerabilities in Popular Media Players

6 0-day Vulnerabilities

0-day vulnerabilities give frequent headaches to developers. System loopholes are often used by hackers even before information about them gets published and vendors release a patch. It’s notable that the number of such vulnerabilities has been increasing in Adobe products: last year it reached 7 (thus, Adobe gave dust to another software giant – Microsoft, which accounts for 5 0-days). Among fresh examples of Adobe flaws, there is a CVE-2011-2462 vulnerability in Adobe Reader detected at the end of 2011 and used to hack ManTech, a contractor of the US Department of Defense.

Table 6. 0-day Vulnerabilities

Application	Vulnerability
Adobe Flash Player	3
Microsoft Internet Explorer	3
Microsoft Windows	2
Adobe Reader	3
Yahoo! Messenger	1
ISC BIND	1
Hancom Office	1

Table 7 provides statistics for 0-days in products from Microsoft and Adobe compared to the total number of vulnerabilities in products from all other vendors.

Table 7. 0-days (Microsoft and Adobe)

Vendor	2006	2007	2008	2009	2010	2011
Microsoft	6	3	5	6	6	5
Adobe	—	—	1	4	7	7
Others	1	—	—	3	—	3

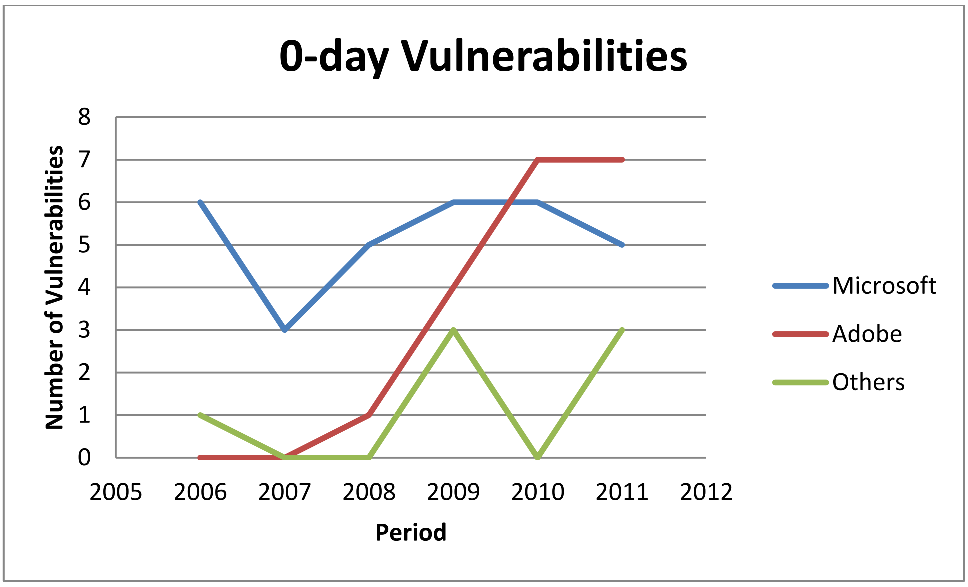

Figure 7. Total Number of 0-days (since 2006)

7 Vulnerabilities in Operating Systems

The wide popularity of Windows adversely affects its security. This Microsoft products contain more vulnerabilities than other operating systems: 92 vulnerabilities were detected in 2011, with two of them being of a critical severity level. However, the greatest number of critical vulnerabilities (33) was detected in Mac OS, while Windows accounted for 22 and various Linux versions, only one. Vulnerabilities in third-party software products were not taken into account in this report.

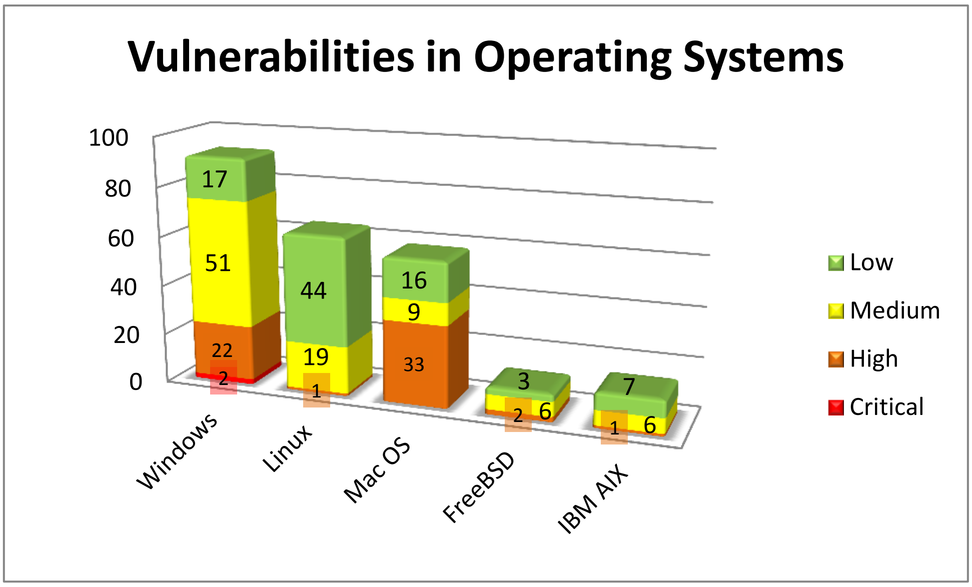

Figure 8. Vulnerabilities in Operating Systems (Severity-Based Distribution)

8 Vulnerabilities in Web Applications

In the segment of web applications, the best conditions for gaining unauthorized access are provided by content management systems (18%). Hackers constantly look for vulnerabilities in them and, as we can see, do find a lot of them (204 vulnerabilities in 2011). When working with sites built on popular platforms, not only should the administrators control suspicious activities, but promptly install every CMS update. The same care should be taken about web forums, which are the second in the list of most vulnerable sources (7%).

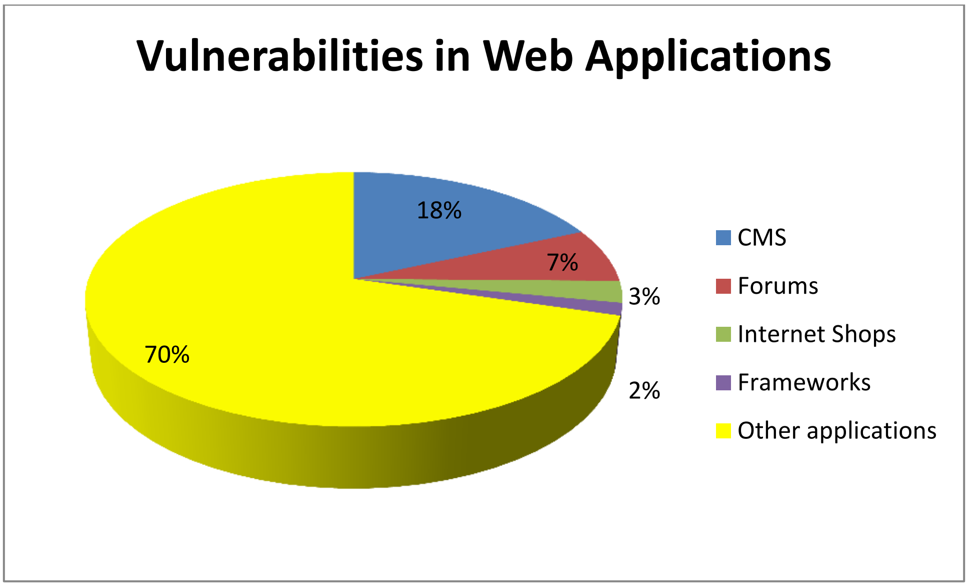

Figure 9. Distribution of Vulnerabilities in Web Applications

9 Reference Materials

Types of Actions

In security notifications, SecurityLab uses the following terms for types of actions:

Brute Force
A type of actions that are performed when an application or an algorithm enables an attacker to guess a user name, password or other data used for access control.

Cross-Site Scripting
A type of actions based on exploitation of vulnerabilities that allow an attacker to manipulate the behavior or content of pages of a web application in the target user's browser. This class includes all vulnerabilities connected to scripting operations in browsers (cross-site scripting o stored and reflected types, cross-site request forgery, HTTP-response splitting, etc.).

Denial of Service
A type of actions based on exploitation of vulnerabilities that allow an intruder to interrupt normal operation of an application or operating system and influence its accessibility.

Sensitive Information Disclosure
A type of actions aimed at detecting vulnerabilities that allow an attacker to gain access to documents, files, credentials, and other sensitive information.

System Data Breach
A type of actions based on exploitation of vulnerabilities that allow an attacker to obtain system data (OS versions, running services, location of the files in the system).

Session Hijacking
A type of actions based on exploitation of vulnerabilities that enable an attacker to hijack a user's session and act as the user.

Unauthorized Data Alteration
A type of actions based on exploitation of vulnerabilities that allow an attacker to alter data without required access privileges, for example, by means of SQL injection.

Escalation of Privileges
A type of actions based on exploitation of vulnerabilities that enable a local user to gain privileges of another account in the system.

Security Restrictions Bypass
A type of actions based on exploitation of vulnerabilities that allow an attacker to bypass certain security mechanisms of an application.

Spoofing Attack
A type of actions based on exploitation of vulnerabilities that allow an attacker to perpetuate identity of another user or system.

System Compromise
A type of actions based on exploitation of vulnerabilities that allow a remote attacker to execute an arbitrary code in the target system with privileges of a user or the vulnerable service.

Severity Level of Vulnerability

In the notifications, SecurityLab estimates the severity level of vulnerabilities according to CVSS v. 2.

Critical Level
This class is assigned to vulnerabilities that allow an attacker to compromise a system remotely without extra actions on the target user's side, and are actively exploited at the moment when they become widely known (0day vulnerabilities). To be considered critical, a vulnerability should rank >= 8.7 according to the CVSS v. 2, and be detected as the result of a security incident.

High Level
This level is assigned to vulnerabilities that allow compromising a system remotely and rank CVSS >= 7.4.

Medium Level
This level is assigned to vulnerabilities that allow triggering denial of service, gaining unauthorized access to data or performing arbitrary code execution (for example, when the user's vulnerable application is being connected to the server captured by the attacker). Their CVSS rating is >= 4.7.

Low Level
Vulnerabilities of this severity level are exploited locally or their exploitation is either hindered or makes little effect on the system (XSS, denial of service of the client application). Their CVSS v. 2 rating is less than 4.7.

10 Positive Research

Our innovation division, Positive Research, is one of the largest and most dynamic security research facilities in Europe. This award-winning centre carries out research, design and analytical work, threat and vulnerability analysis and error elimination. Our experts work alongside industry bodies, regulators and universities to advance knowledge in the field of information security and to assist in the development of industry standards. Naturally, this knowledge is also applied to improving the company's products and services.

Positive Research identifies over 100 0-day vulnerabilities per year in leading products such as operating systems, network equipment and applications. It has helped manufacturers including Microsoft, Cisco, Google, SAP, Oracle, Apple, and VmWare to eliminate vulnerabilities and defects that threatened the safety of their systems.