OWASP-EAS

ENTERPRISE APPLICATION SECURITY

SAP SECURITY IN FIGURES

A GLOBAL SURVEY 2007–2011

Authors:

Alexander Polyakov
Alexey Tyurin

Other contributors:

Dmitry Chastukhin

Dmitry Evdokimov

Evgeniy Neyolov

Alina Oprisko

Content

Important notes

The partnership agreement and relationship between aouthors and SAP prevents us from publishing the detailed information about vulnerabilities before SAP releases a patch. This whitepaper will only include the details of those vulnerabilities that we have the rights to publish as of the release date. However additional examples of exploitation that prove the existence of the vulnerabilities can be seen in conference demos as well as at http://erpscan.com [1].

Moreover, our research in the field of SAP Security surveys and other areas of SAP security does not end with this whitepaper. You can find the latest updates about the statistics of SAP services found on the Internet at http://sapcan.com [2].

The survey was conducted by authors as part of contribution to the OWASP-EAS non-profit organization, which is focused on Enterprise Application Security awareness.

1. Intro

ERP system is the heart of any large company; it enables all the critical business processes, from procurement, payment and transport to human resources management, product management and financial planning. All data stored in ERP systems is of great importance and any illegal access can mean enormous losses, potentially leading to termination of business processes. In 2006 through 2010, according to the Association of Certified Fraud Examiners (ACFE), losses to internal fraud constituted 7 % of yearly revenue on average [3]. This is why we decided to increase awareness in this area.

Losses to internal fraud constituted 7 % of yearly revenue on average.

The wide-spread myth that ERP security is limited to SOD matrix has been dispelled lately and seems more like an ancient legend now. Within the last 5 years, SAP security experts have spoken a great deal about various attacks on SAP from RFC interface, SAPROUTER, SAP WEB and SAP GUI client workstations [4]. Interest in the topic has been growing exponentially: in 2006, there was 1 report [5] on SAP at the technical conferences dedicated to hacking and security, whereas in 2011 there were more than 20 of them already. A variety of hack tools has been released that prove the possibility of SAP attacks [6], [7], [8].

According to the statistics of vulnerabilities found in business applications, there were more than 100 vulnerabilities patched in SAP products in 2009, while it grew to more than 500 in 2010. By March, 2012, there are more than 2000 SAP Security notes about vulnerabilities in various SAP components.

Most of these vulnerabilities allow an unauthorized user to gain access to all the critical business data, so it is necessary to think about the main attack vectors and the ways to secure those highly critical systems.

1.1. Corporate security changes

The development of corporate infrastructure tends to move from a decentralized model towards integration of business processes into united systems. Not long ago, there would be several servers in a company, including mail server, file server, domain controller, etc. However, these functions have been integrating into a united business application, resulting in more convenient access but also in a united failure point. Business applications and ERP systems store all critical company data, from financial reports and personal information to lists of contractors and corporate secrets. Such a system would be the main target of an insider or an external attacker, and their ultimate aim is nowhere near administrative access to the domain controller.

Nevertheless, many information security officers are, unfortunately, scarcely informed about the security of business applications like SAP. Another problem is that the function of providing security lies on the owner of a system rather than the CISO, and owners only respond to themselves. In the end, nobody is responsible for the security of the most critical system elements.

Less global problems are, for example:

- **Lack of qualified specialists** – SAP specialists in most companies think of SAP security as SOD matrix only, whereas CISOs understand SAP threats scarcely at best, not to mention advanced tweaks.

- **Great range of advanced configuration** – There are more than 1000 parameters in the standard system configuration, plus a great range of advanced options, not to mention segregation of access rights to various objects like transactions, tables, RFC procedures etc. For example, web interfaces for the access to the system alone can amount to several thousands. Providing the security of a configuration of this scale can be hard even for a single system.

- **Customizable configuration** – There are no two similar SAP systems because most parameters are customized for every client in one way or the other. Furthermore, individualized programs are developed and their security is to be accounted for, too, in a complex assessment.

The purpose of this report is to show a high level view of SAP Security in figures so that the problem area is not just theoretically comprehensible but based on actual numbers and metrics – from the information about the number of found issues and their popularity to the number of vulnerable systems, all acquired as a result of a global scan [2].

2. Vulnerability statistics

The information about vulnerabilities in SAP by their popularity, criticality and the affected systems is given here. The top 5 most valuable publicly known vulnerabilities are presented as well.

2.1. Number of SAP Security notes

SAP occasionally releases an internal advisory called SAP Security note. Such an advisory usually stores information about one or more vulnerabilities found in SAP products or misconfigurations that bear some risk to SAP systems. The first SAP Security note was published in 2001 and since 2007 the number of published notes began to grow exponentially.

As of April 26, 2012, more than 2000 SAP Security notes have been published.

During 2011, the approximate number of SAP Security notes published every month on the Critical Patch Day (every second Tuesday) was about 65. In comparison to other software vendors that is more than Microsoft, Oracle or Cisco. Needless to say, just 3 years ago this number was much lower.

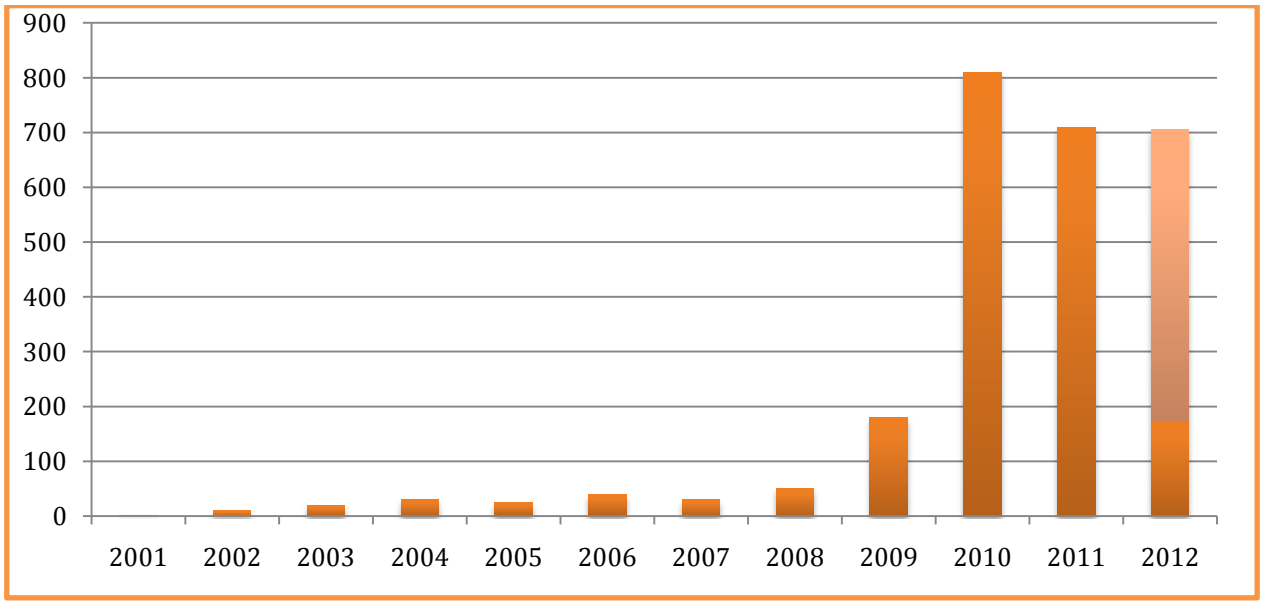


Figure 2.1-1 Number of Sap Security notes per year.

**The data presented in this picture was collected on April 26, 2012, when a total of 2027 notes had been published.*

2.2. SAP Security notes by criticality

SAP has 5 different levels of criticality for published notes:

1 – HotNews
2 – Correction with high priority
3 – Correction with medium priority
4 – Correction with low priority
6 – Recommendations/additional info

Most of the issues (69%) have high priority, which means that about 2/3 of the published vulnerabilities must be corrected quickly.

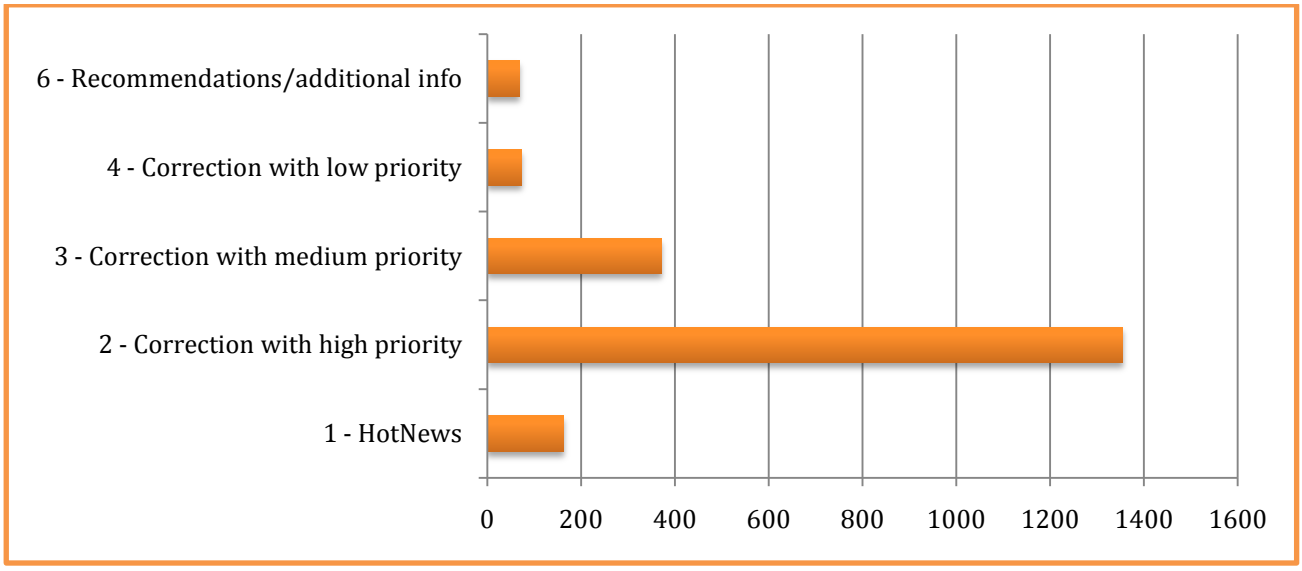


Figure 2.2-1 Number of Sap Security notes by criticality level.

2.3. SAP Security notes by type

All published SAP Security notes were analyzed by their popularity. Most popular types of issues are presented below:

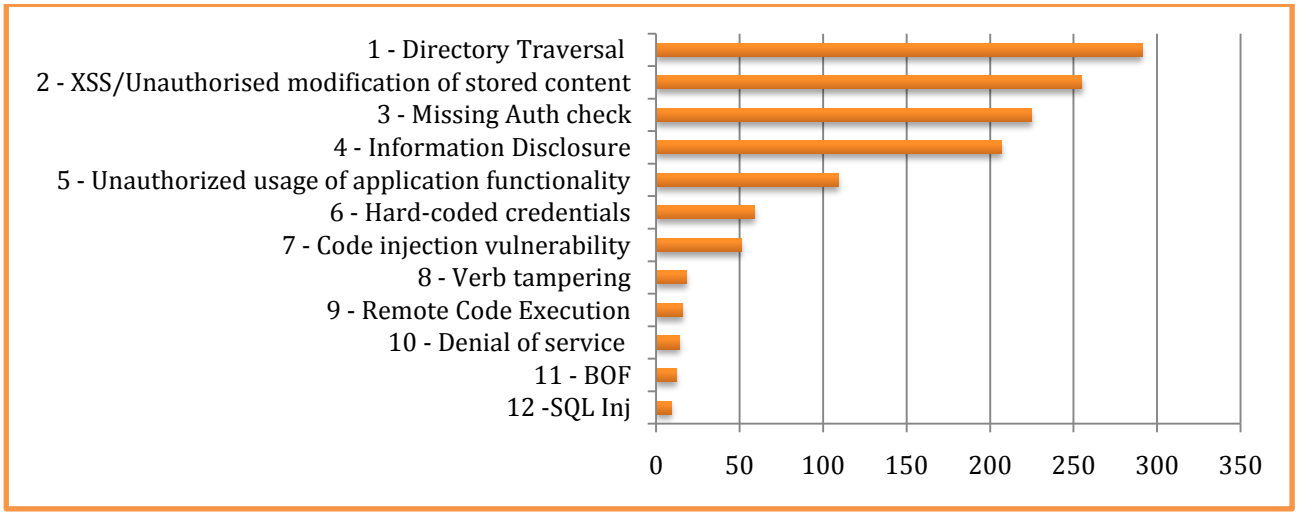


Figure 2.3-1 SAP Security notes by type

Note that the new type of vulnerability called Verb Tampering [9], which was first discovered by ERPScan, became one of the most popular vulnerabilities of all time. A total of 18 issues have been found.

About 20% of found vulnerabilities are not presented in the top 12 because many unique issues exist in SAP systems. Some of them may be found in our presentation called "Top 10 most interesting SAP vulnerabilities and attacks" [10].

**The data presented in this picture was collected on April 26, 2012, when a total of 2027 notes had been published.*

2.4. Number of acknowledgements to external researchers

In 2010, SAP decided to give acknowledgements to external security researchers for the vulnerabilities found in their products. In the figure, you can see the number of vulnerabilities that were found by external researchers since 2010. Half of the vulnerabilities were found and successfully patched by SAP with the help of ERPScan (50 vulnerabilities and 26% of all) and VirtualForge (44 vulnerabilities which is 23% of all). The remaining 51% of vulnerabilities were discovered by 20 additional companies and the number of new companies is continuing to grow, proving that this topic is growing in popularity [11].

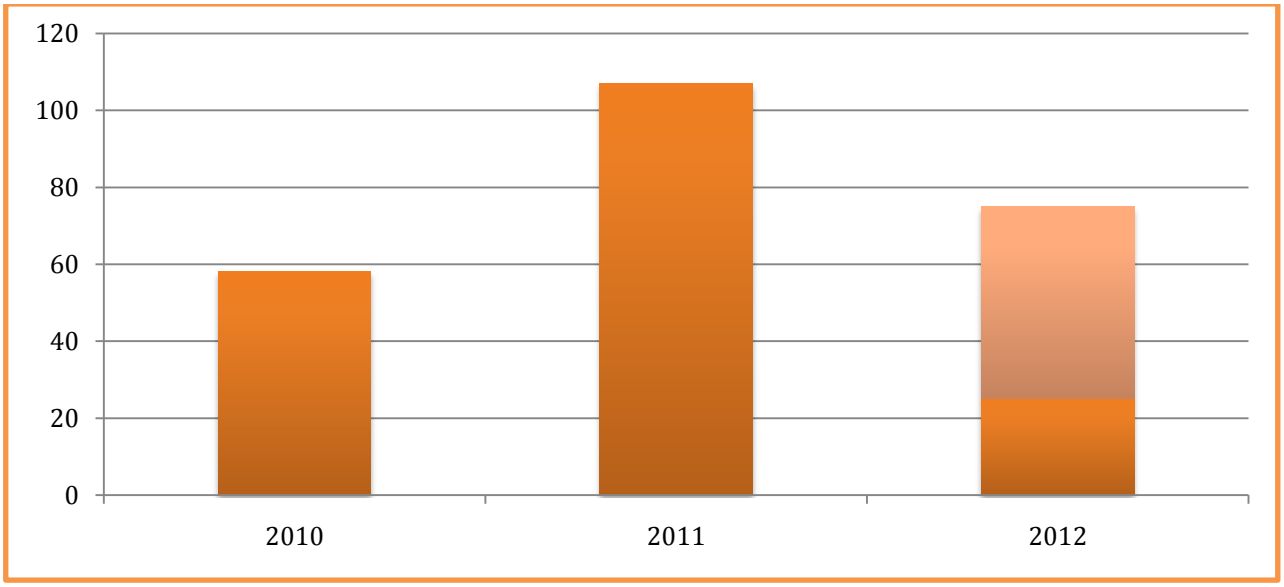
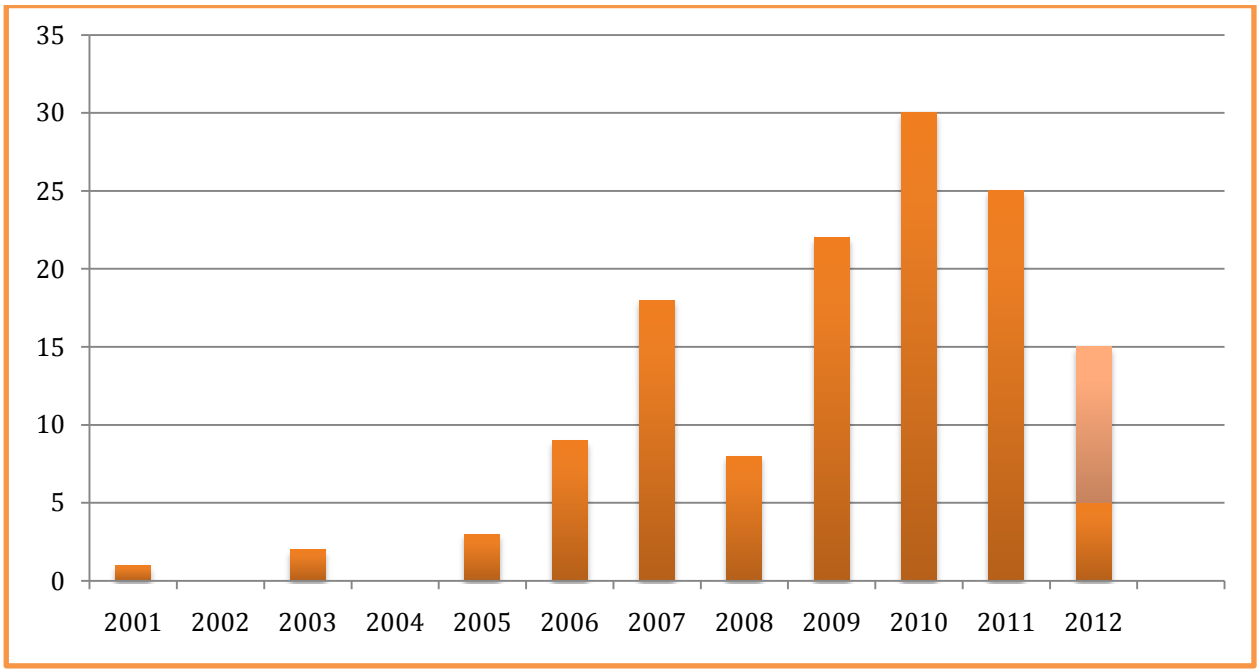


Figure 2.4-1 Number of acknowledgements to external researchers by year

2.5. Amount of publicly available information

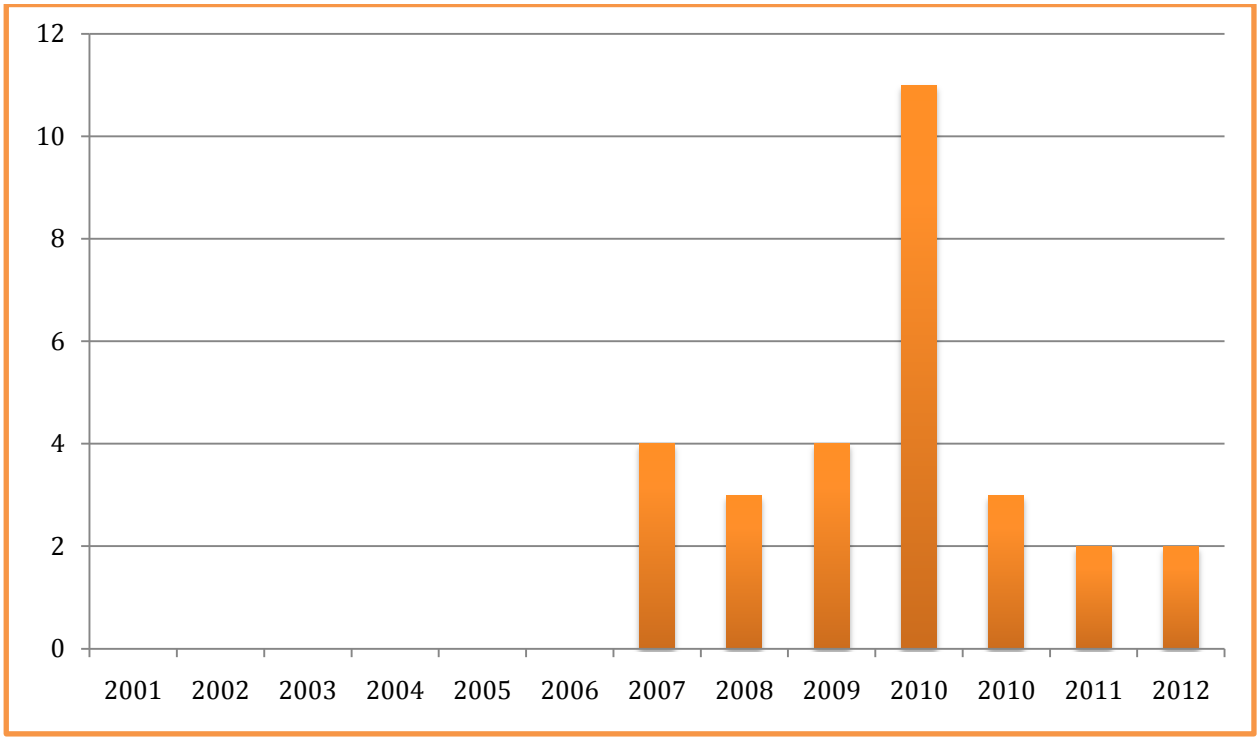
The most critical threat is connected to the vulnerabilities which contain information about the methods of exploitation (detailed advisories, POC codes and working exploits) publicly available. Information was gathered from 2 most popular sources:

SecurityFocus [13] – Detailed advisories, sometimes with POC code, can usually be found here. All the vulnerabilities published here have high probability of exploitation. ***123 vulnerability advisories were found there*** (6% of all vulnerabilities).



Pic 2.5-1 Advisories by year

Exploit-DB [14] – Usually, exploit codes that can be 100% used without any modification and additional knowledge of exploiting systems can be found here. All the vulnerabilities published here have critical probability of exploitation. ***A total of 24 exploits were found here*** (1% of all vulnerabilities).



Pic 2.5-2 Exploit by year

In the picture below you can find vulnerabilities categorized by probability and ease of exploitation according to the amount of information available to hackers at public sources, as opposed to classified information from SAP Security notes.

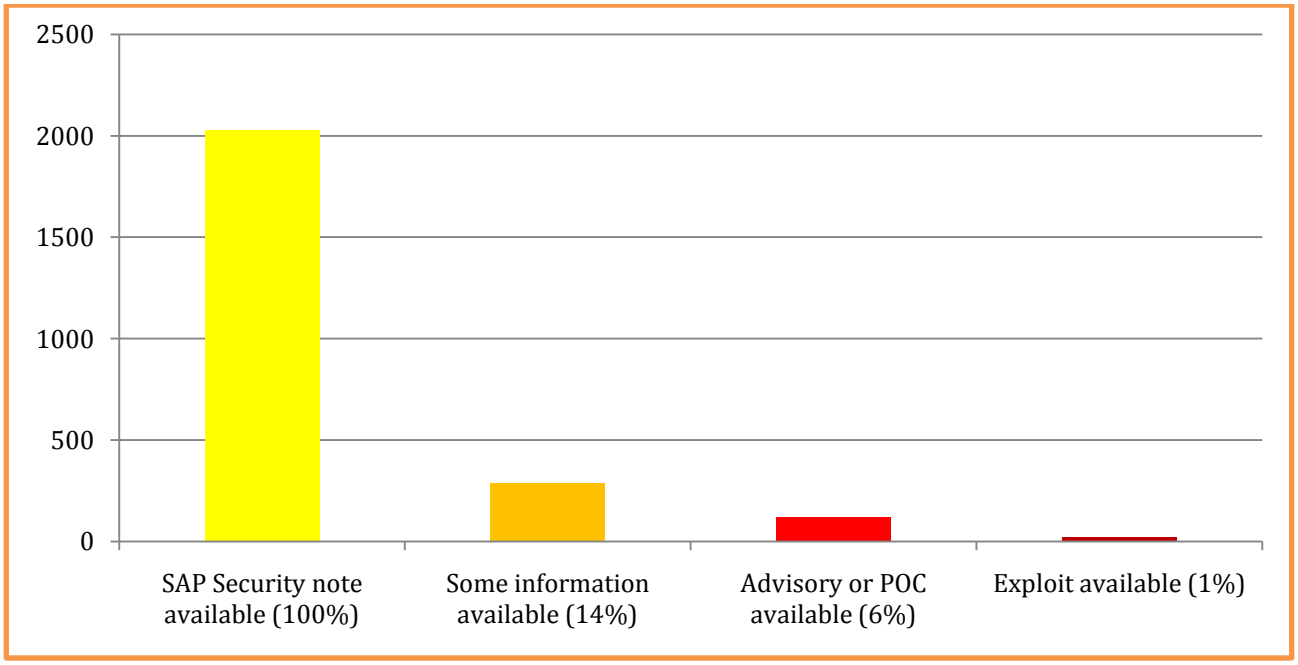


Figure 2.5-1 SAP vulnerabilities by probability and ease of exploitation

2.6. Top 5 most valuable vulnerabilities in 2011

Out of the many published vulnerabilities, we have chosen the top 5 with the most significant threats published in 2011:

- Authentication bypass through Verb Tampering [15]
- Authentication bypass through the Invoker servlet [16], [17]
- Buffer overflow in ABAP Kernel call [18]
- Remote code execution via TH_GREP [19]
- JSESSIONID disclosure through SAP Management console [20]

1. Authentication bypass through Verb Tampering

The vulnerability was found in the J2EE engine of SAP NetWeaver allows an anonymous attacker to fully compromise a SAP system. Approximately 40 different SAP applications vulnerable to this attack were found. The most critical one allows creating any user, assigning him any role in the system and executing any OS command.

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	Anonymously through the Internet
Ease of exploitation:	Easy
CVSSv2:	10
Advisory:	http://erpscan.com/advisories/dsecrg-11-041-sap-netweaver-authentication-bypass-verb-tampering/
Patch:	Sap notes: 1589525, 1624450
Author:	Alexander Polyakov (ERPScan)

2. Authentication bypass through the Invoker servlet

The vulnerability was found in the J2EE engine of SAP NetWeaver allows an anonymous attacker to bypass security restrictions of SAP web services and directly call critical functions by their class names. Approximately 30 different applications are vulnerable to this attack. Depending on the vulnerable application, it is possible to add new users into the system, read OS files including database files or disclose critical information.

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	Anonymously through the Internet
Ease of exploitation:	Easy
CVSSv2:	10
Advisory:	http://help.sap.com/saphelp_nw70ehp2/helpdata/en/bb/f2b9d88ba4e8459 e5a69cb513597ec/frameset.htm
Patch:	SAP note 1585527
Author:	SAP

3. Buffer overflow in ABAP Kernel call

The buffer overflow vulnerability was found in the ABAP Kernel call. It can be exploited by calling the ABAP Report which uses a vulnerable Kernel call and transmits user's input into it. The vulnerability allows an authenticated user with BASIS rights to compromise the OS and execute any command with the rights of the <SID>adm user. We have created a working exploit in our lab, however, only a PoC exploit is currently available to the public.

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	A user with BASIS rights is needed
Ease of exploitation:	Medium. Good knowledge of exploit writing for multiple platforms is necessary
CVSSv2:	4.8
Advisory:	http://virtualforge.com/tl_files/Theme/whitepapers/BlackHat_EU_2011_Wiegenstein_The_ABAP_Underverse-WP.pdf
Patch:	Sap note 1487330, 1529807
Author:	Andreas Wiegenstein

4. Remote code execution via TH_GREP

Remote command execution vulnerabilities in ABAP became popular during 2011. One of the best known vulnerabilities was found in the TH_GREP function module. It is an interesting fact that the vulnerability was found and patched in 2010 by Joris but after analyzing the patch our researcher Alexey Tyurin found that the patch was implemented incorrectly and that it was possible to bypass it on the Windows OS. So finally this vulnerability was patched. This vulnerability allows an authenticated user with BASIS rights to compromise the OS and execute any OS command with the rights of <SID>adm user.

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	A user with BASIS rights is needed
Ease of exploitation:	Medium. Good knowledge of exploit writing for multiple platforms is necessary
CVSSv2:	6
Advisory:	http://erpscan.ru/advisories/dsecrg-11-039-sap-netweaver-th_grep-module-code-injection-vulnerability-new/
Patch:	SAP note 1620632
Author:	Joris van de Vis and Alexey Tyurin (ERPScan)

5. JSESSIONID disclosure through the SAP Management console

A vulnerability was found in SAP MMC service by Mariano Nunez which allow anonymous reading of any log file from SAP. During our research, while performing penetration tests on SAP systems, we found that sometimes log files can store the JSESSIONID value, if the trace level is set to maximum. With access to JSESSIONID, it is possible to insert it in a cookie file and log into SAP Portal as an existing user.

Espionage:	High
Sabotage:	Medium
Fraud:	High
Availability:	Medium. Remotely enabled access to MMC
Ease of exploitation:	Medium. Trace must be ON
CVSSv2:	5.6
Advisory:	http://erpscan.com/wp-content/uploads/2012/06/Top-10-most-interesting-vulnerabilities-and-attacks-in-SAP-2012-InfoSecurity-Kuwait.pdf
Patch:	Sap note 1439348
Author:	JSESSIONID vector found by Alexey Tyurin (ERPScan)

3. Growing interest

While most of the security trends and possible threats are focused on mobile, cloud, social networks and critical infrastructure which will potentially have threats in near future, there is a topic called ERP security and threats to those systems exist now. That's why the number of companies which are focused on ERP security and which sell software for its assessment is growing. So the number of security consulting companies that try to sell special consulting services for ERP security is growing as well.

3.1. Number of security reports in technical conferences

Since 2006, SAP security begins to receive a lot of attention in technical security conferences like BlackHat, HITB and others. Since 2010, this trend expands to other conferences; more and more companies and researchers begin to publish their research in the field of SAP security. In 2006–2009, talks were mostly focused on showing typical information security threats in SAP landscapes such as SAP web application security, SAP client-side security, SAP backdoors and Trojans. The last year was focused on specific research of different types of vulnerabilities in SAP and ABAP code and Kernel, like SQL Injections [21], Buffer Overflows [18], vulnerabilities in the J2EE engine like Verb Tampering [15], Session Fixation [22], Invoker Servlet [9], and the security of SAP's own protocols such as DIAG [23] and P4 [9].

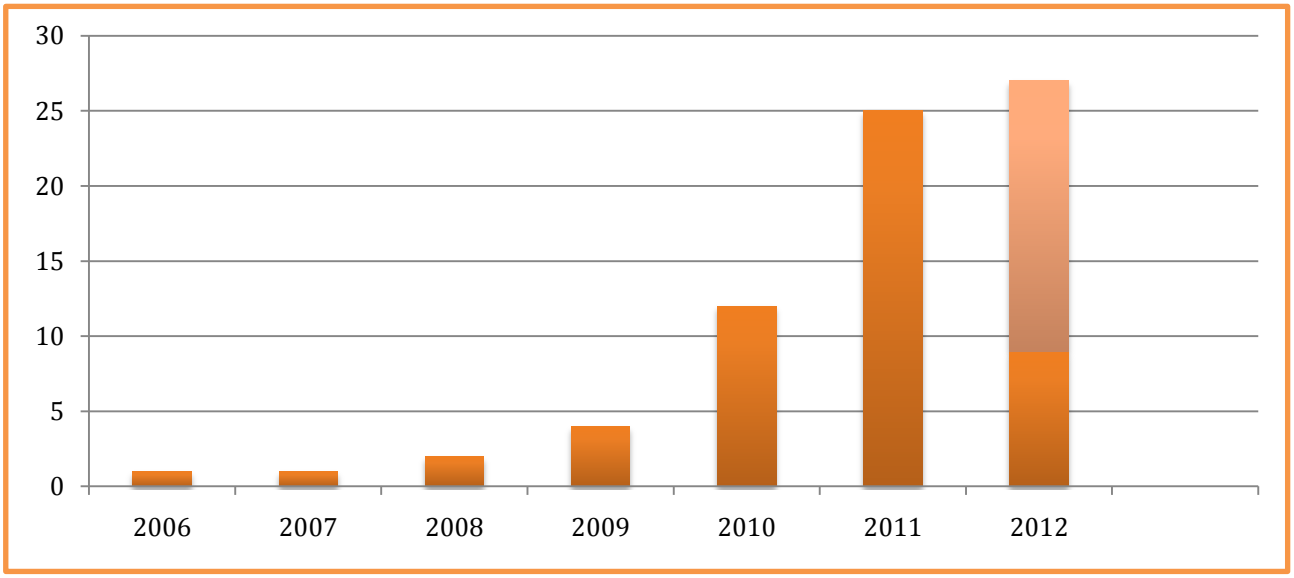


Figure 3.1-1 Number of SAP security talks presented at different conferences by year

Number of SAP security talks presented in different conferences every year is shown in the slides. For 2012, an approximate number is estimated based on the first 4 months.

**Data was collected from different conference websites as of April 26, 2012*

4. SAP on the Internet

Among many people who work with SAP, a popular myth is that SAP systems are inaccessible from the Internet, so all SAP vulnerabilities can only be exploited by an insider.

Excerpt from an Interview with Sachar Paulus for CIO magazine [24].

(SVP of product and security governance at SAP)

CSO: **What are some of the biggest ERP security threats? What are SAP's biggest software security challenges?**

Sachar: The other **threat comes from people connecting their ERP systems to the Internet**, either to extend the supply chain support of the system or to expose specific functionalities in order to make life easier for the employees. The problem with this is that the classical, well understood **Internet threats are often not understood by the ERP people**. The people who are responsible for ERP understand the insider threat because they have dealt with it for years, but when there is a demand from his business to extend systems to the Internet, **they don't think about threats like cross-site-scripting**. Viruses or worms using the ERP platform may come into play, and they don't sufficiently understand the importance of security patches. This is a huge challenge to the organization. **It needs to bring together people who understand ERP security, and people who understand Internet, e-mail and Web services security.**

Business applications are not only Accessible internally; this myth comes from 10 years ago when mainframes were prevalent. Business is changing and companies want to have their applications connected. They need to connect to departments worldwide, share data with clients via web portals, SRM and CRM systems and get access from any place with mobile solutions.

Almost all business applications have web access now.

This part of the report is destined to destroy the myth by showing how many companies make which services available for remote access, how those services are vulnerable to the latest threats.

4.1. Google search results by country

These statistics were collected using the well-known Google search requests [25].

Application server type	Search string
SAP NetWeaver ABAP	Inurl:/SAP/BC/BSP
SAP NetWeaver J2EE	Inurl:/irj/portal
SAP BusinessObjects	inurl:infoviewapp

As a result of the scan, about 610 unique servers with different SAP web applications were found. The J2EE server seems to be the most popular platform. Unfortunately, this server is more vulnerable than the ABAP engine, having at least 3 different vulnerabilities that can be executed anonymously and give full access to the system. On the other hand, the ABAP engine has numerous default users [26] that can be used by attackers. SAP BusinessObjects server has both problems.

Application server	Number	%
SAP NetWeaver J2EE	268	44%
SAP Web Application Server	163	27%
SAP BusinessObjects	106	17%
SAP NetWeaver ABAP	73	12%

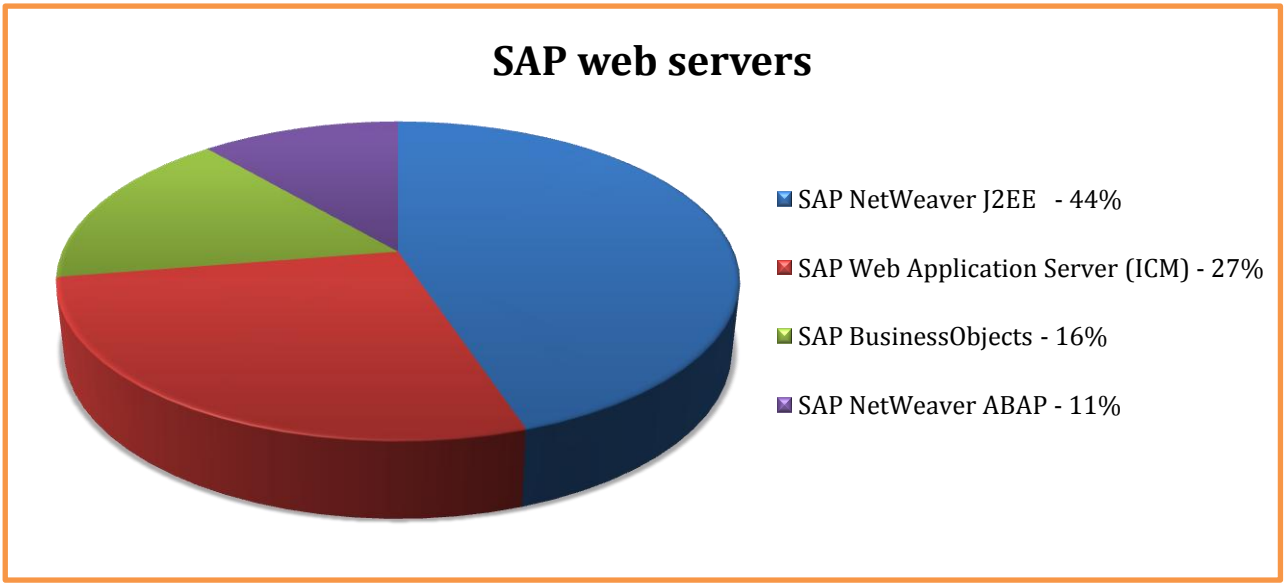


Figure 4.1-1 SAP Application servers by type

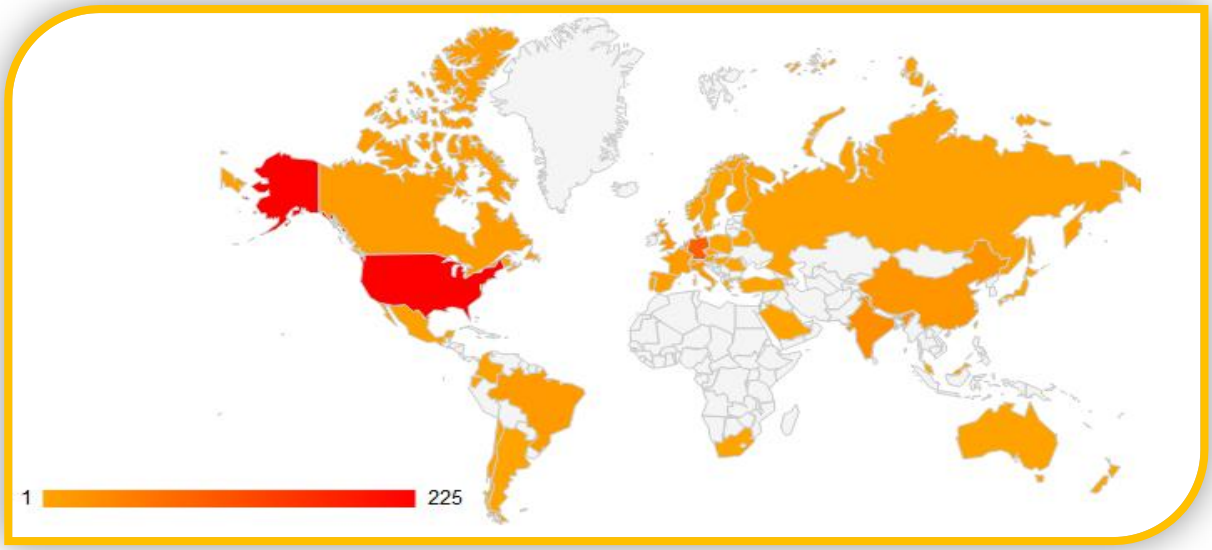


Figure 4.1-2 SAP Application servers by country

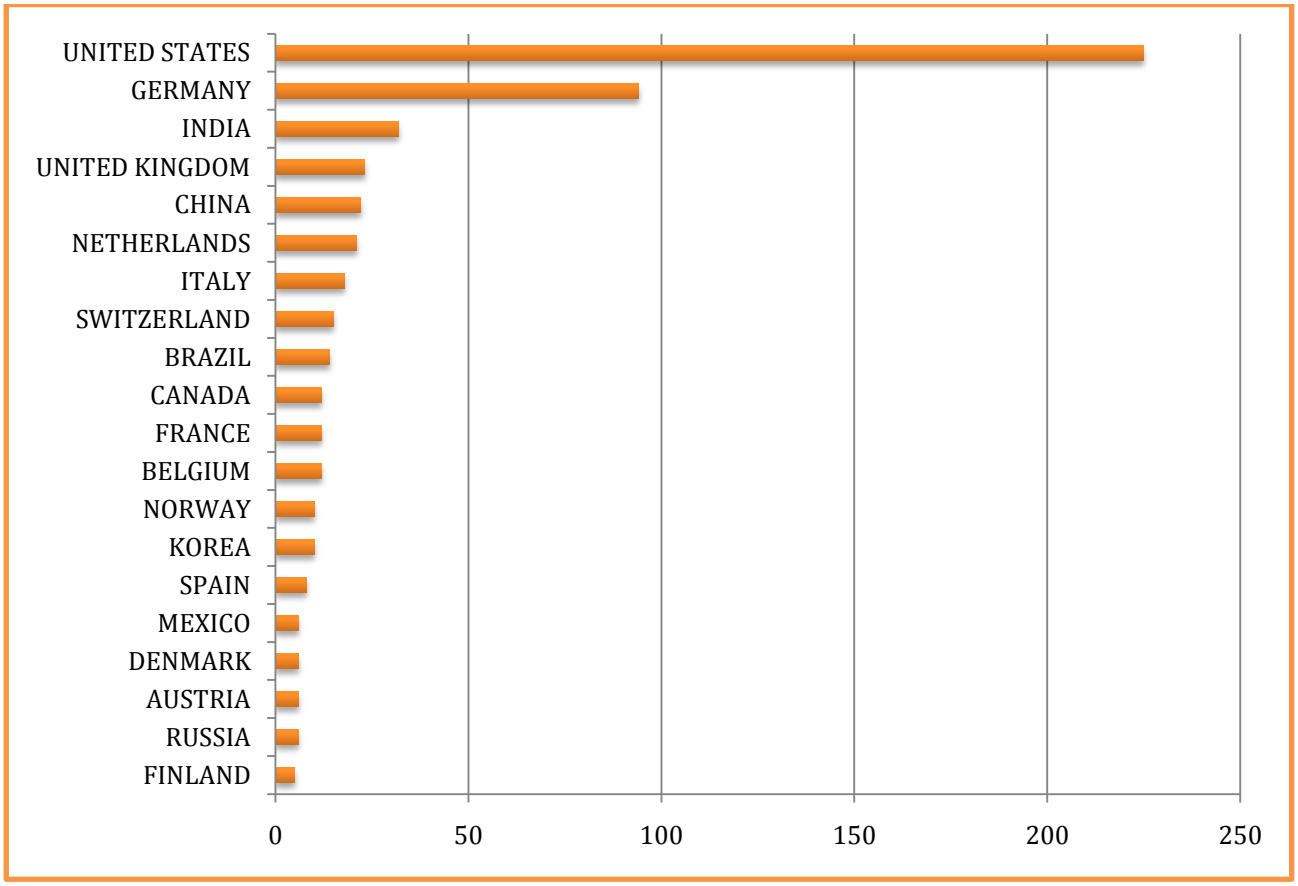


Figure 4.1-3 Overall number of SAP Application servers found in Google, sorted by country (top 20)

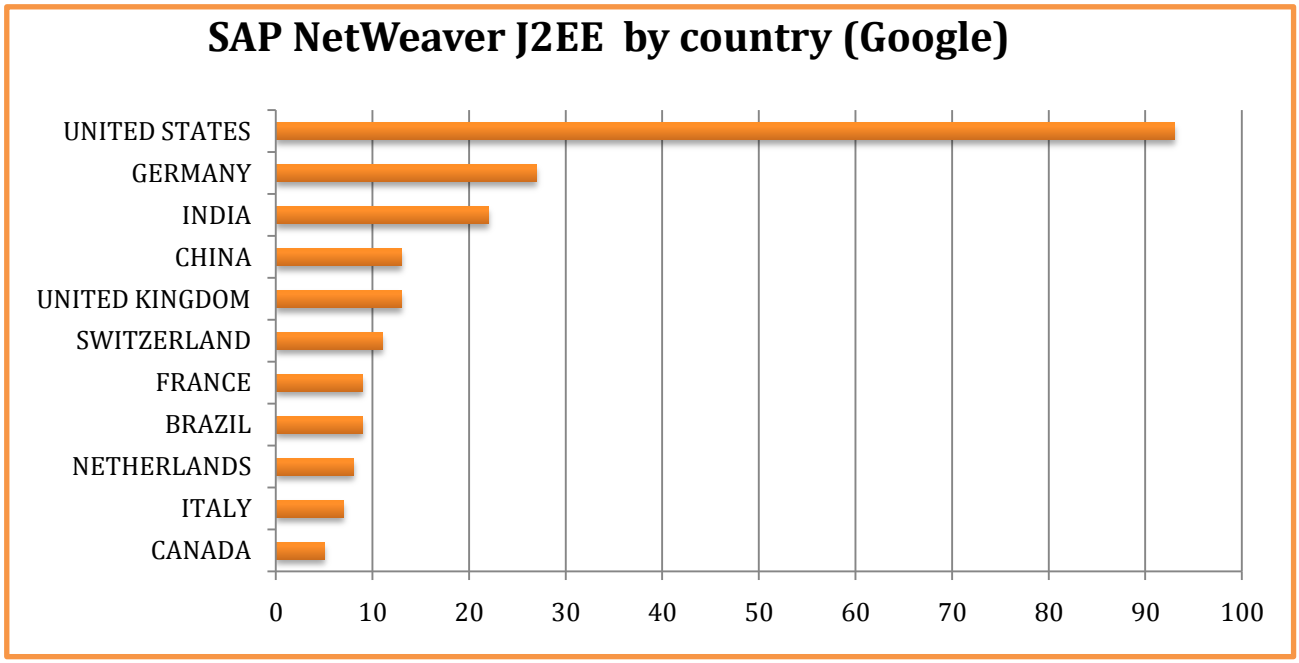


Figure 4.1-4 Overall number of SAP NetWeaver J2EE servers found in Google, sorted by country (top 10)

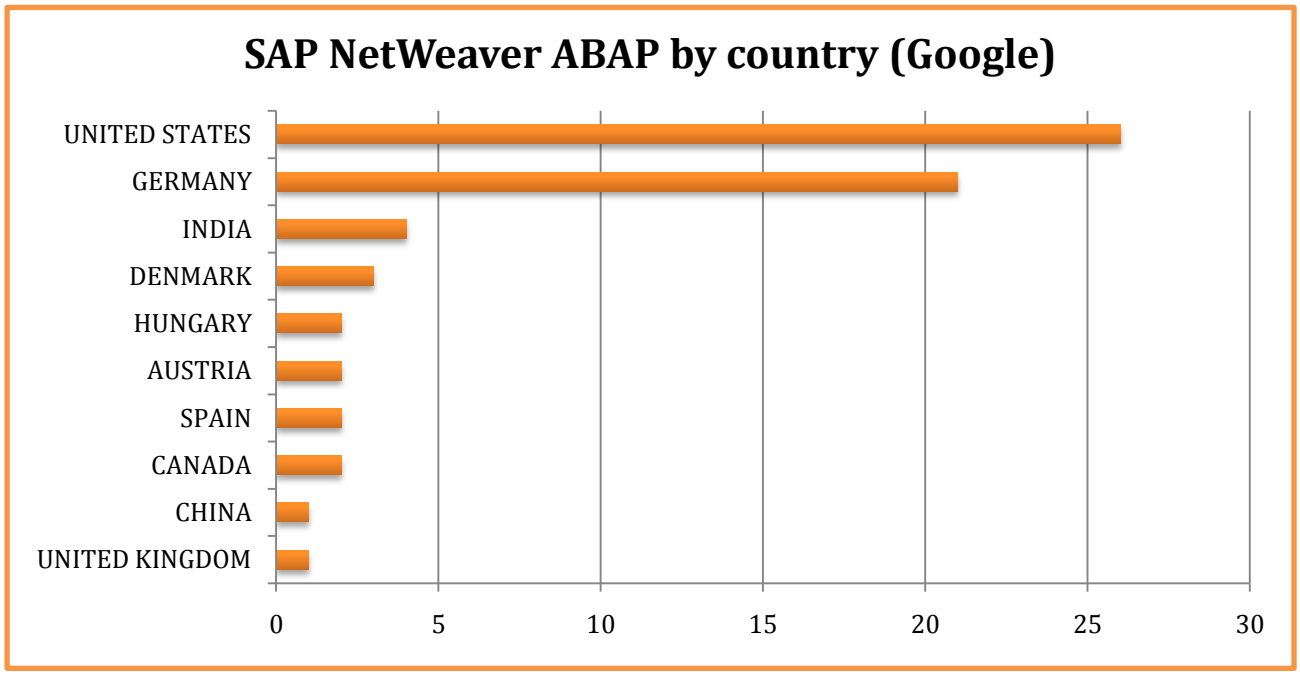


Figure 4.1-5 Overall number of SAP NetWeaver ABAP servers found in Google, sorted by country (top 10)

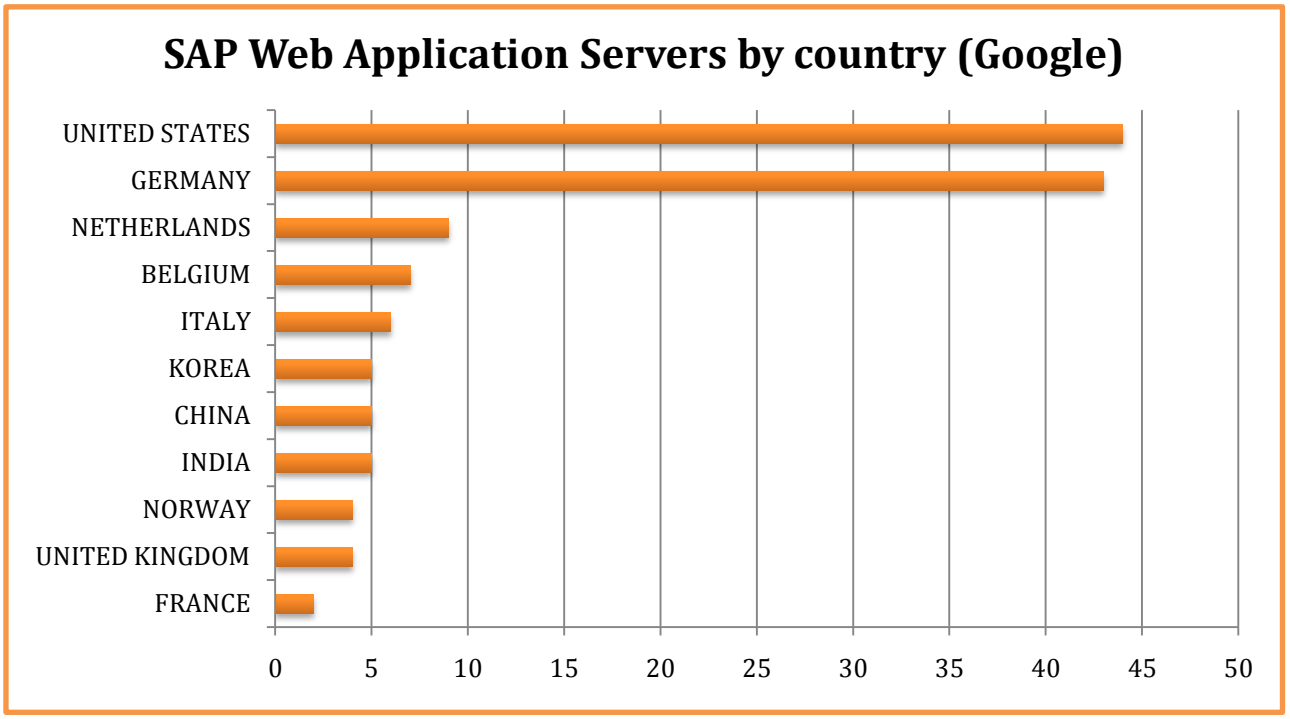


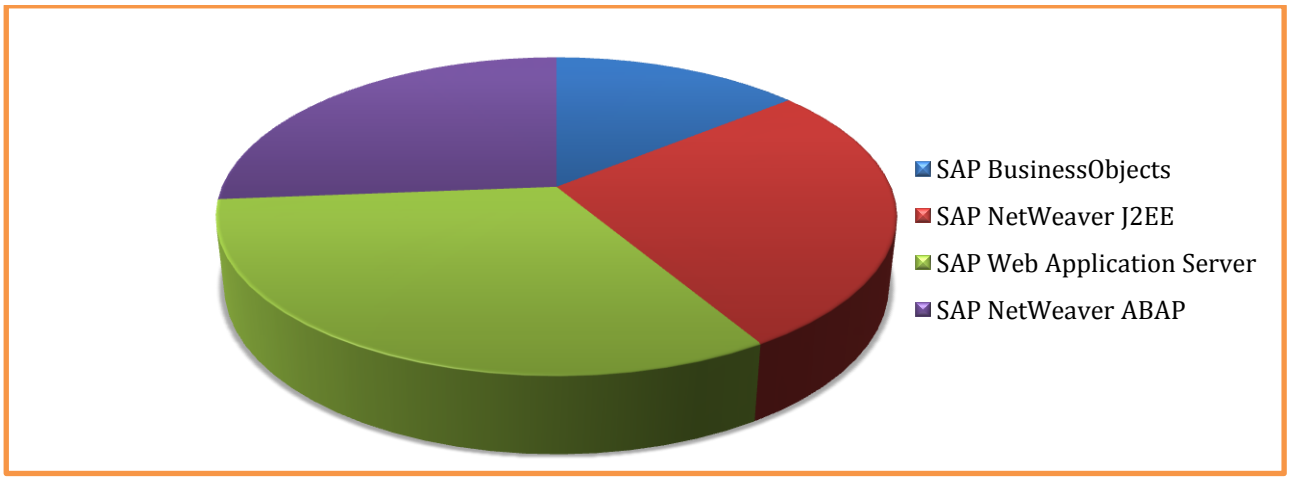
Figure 4.1-6 Overall number of SAP WebAS servers found in Google, sorted by country (top 10)

4.2. Shodan search results by country

Another source which can help to find SAP web interfaces available on the Internet is called www.shodanhq.com. The difference is that this service not only finds those applications which were "crawled" by web spiders but it scans the whole Internet for the 80th port (others, too) and can be used for finding more SAP systems.

A total of 2677 servers with different SAP web applications was found and it is 4.5 times more than using Google search.

Application server	Number	%
SAP Web Application Server	863	32%
SAP NetWeaver J2EE	734	27%
SAP NetWeaver ABAP	686	26%
SAP BusinessObjects	394	15%



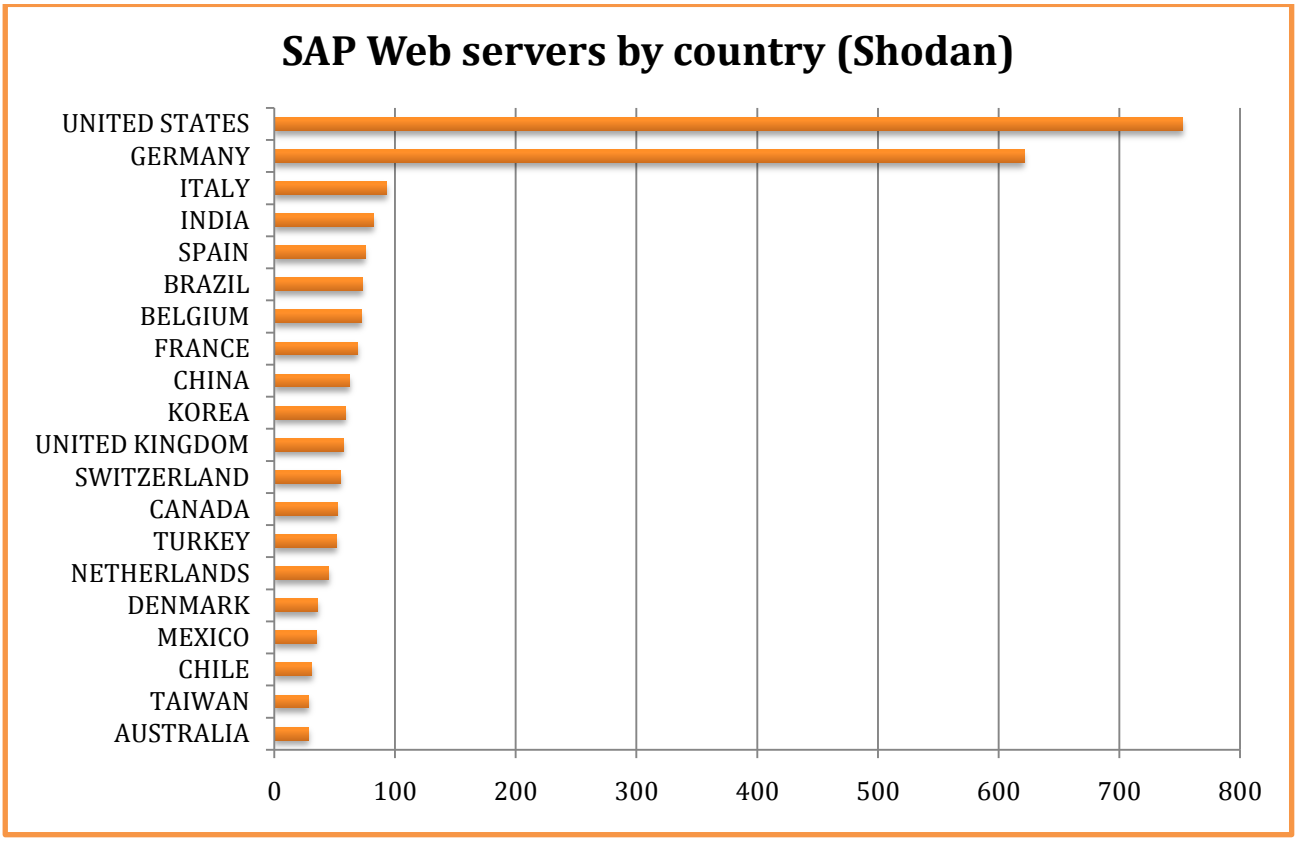


Figure 4.2-1 Overall number of SAP Application servers found in Shodan, sorted by country (top 20)

4.3. Portscan search result by country

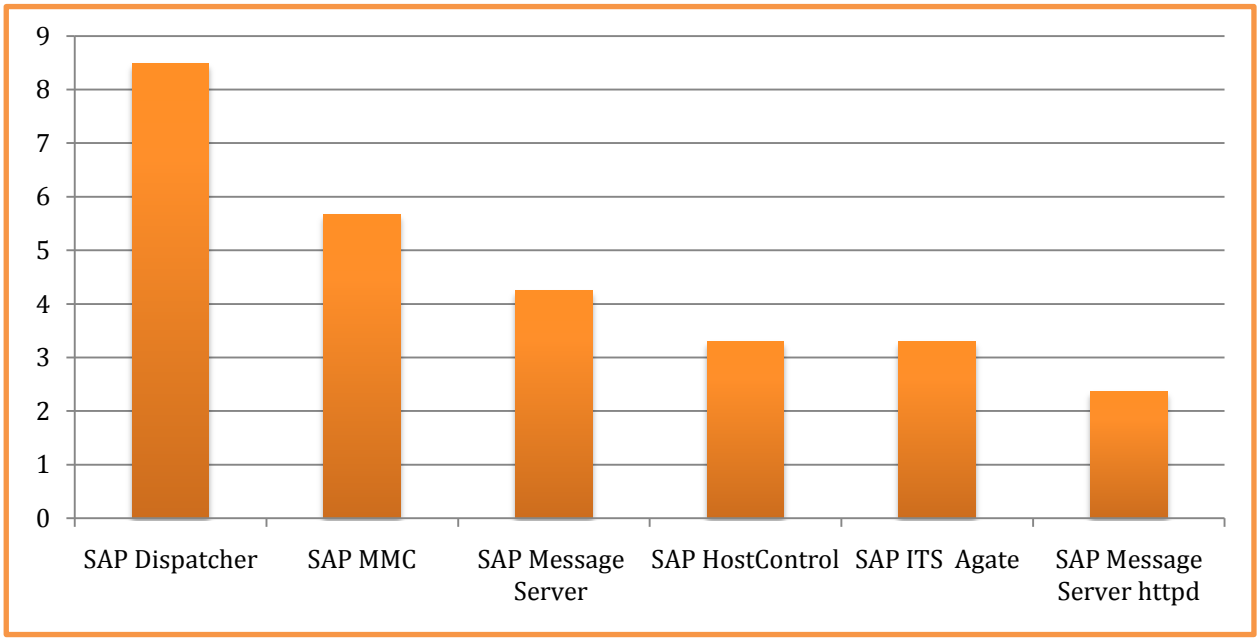
The most interesting and complex research was performed by scanning the Internet not only for web services but also for services which shouldn't be accessible from the Internet.

At first stage, it has been performed with a simple algorithm which only scans subnets of the servers that were found during Google and Shodanhq scan (about 1000 subnets in total). Many ports were found which are listened by SAP Applications such as Message Server HTTP, SAP Gateway, SAP HostControl.

Another project which is still in process is a global internet scan for open ports. As an example here are published results collected from Germany. Total there were found 212 SAP Routers in Germany installed on default port 3299. After obtaining a list of SAP routers a scan was processed among all sub networks where SAPRouters were found. During the scan information about publicly available SAP services such as SAP Hostcontrol, SAP Dispatcher, SAP Message Server, SAP Management console were collected.

In the picture you will find a percentage of German companies that expose their unnecessary SAP services to Internet. The number of open ports will be updated online on the http://sapscan.com – official site of this project.

8% of German companies that use SAP, expose critical services like Gateway or Dispatched directly to the internet bypassing SAP Router security.



Pic 4.3-1 Percent of companies in Germany that expose critical SAP services to Internet.

5. SAP versions

We have checked the major versions of the ABAP and J2EE engines which were found on the Internet to understand the lifecycle of released products and to know which version is the most popular now. We have also checked the popularity of OS and RDBMS which are used with SAP.

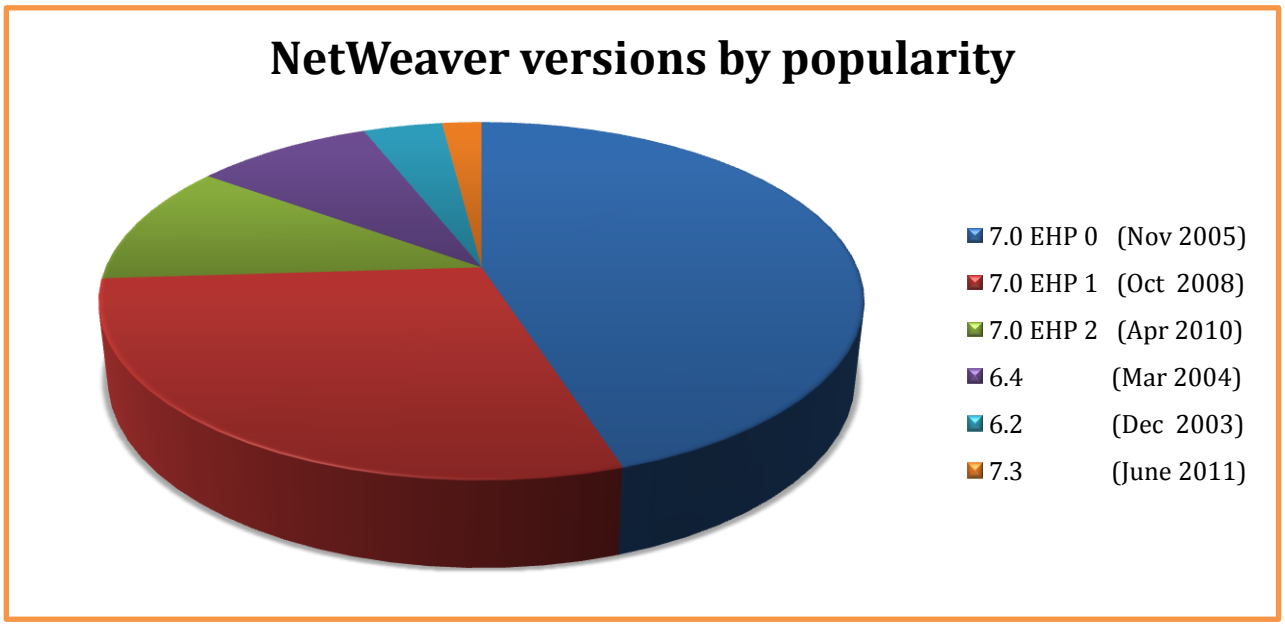
5.1. ABAP engine versions

ABAP versions were collected by connecting to the root of an application server and parsing the HTTP response methods. We also used information disclosure vulnerability. Information about SAP NetWeaver version can easily be found if the application is configured insecurely so that it allows an attacker to get information from the /sap/public/info url.

After scanning all the available SAP NetWeaver ABAP servers, it was found that 59% of them are vulnerable to information disclosure.

The most powerful security options, like disabling access to all BSP, are installed by default in EHP 2, and EHP 2 is only installed on 11% of all servers. This means that even if SAP cares about the security of their systems, the best part of securing SAP systems lies on administrators.

Most popular release (45%) – NetWeaver 7.0 and it was released in 2005!

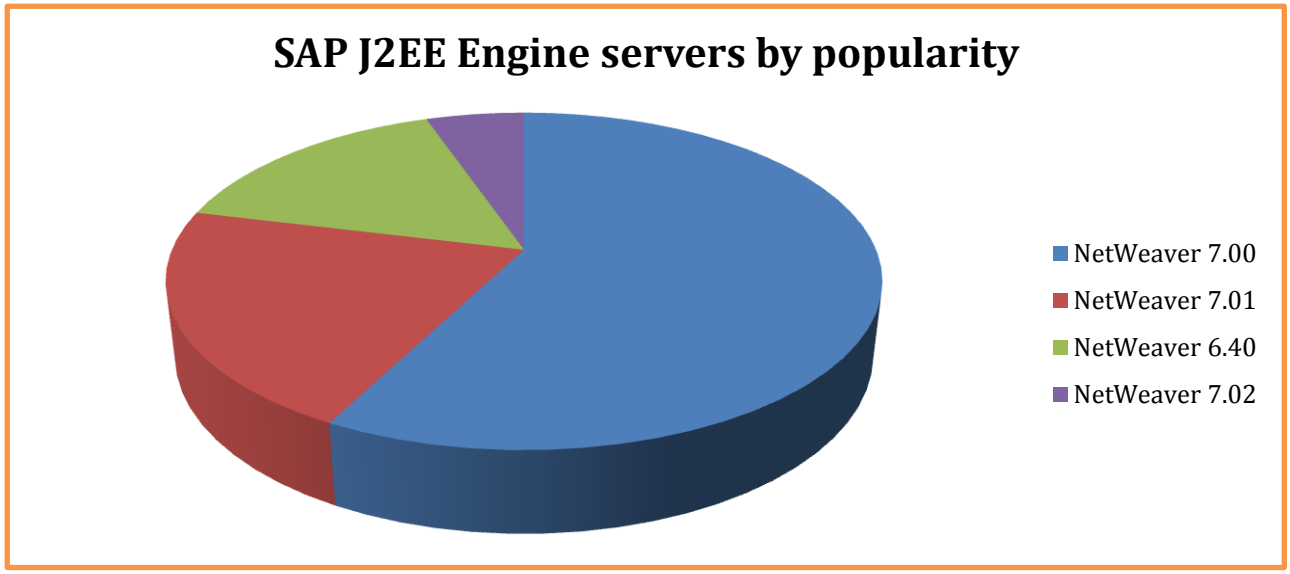


5.2. J2EE engine versions

The information about the version of the J2EE engine can be easily found by reading an HTTP response. However, detailed info about the patch level can be obtained if the application server is not securely configured and allows an attacker to get information from some pages. As an example, there are at least 2 pages that disclose the information about the J2EE engine: /rep/build_info.jsp and /bcb/bcbadmSystemInfo.jsp [27], [28].

After scanning all the available SAP NetWeaver J2EE servers, it was found that 62% of them are vulnerable to the /bcb/bcbadmSystemInfo.jsp information disclosure page and 17% to /rep/build_info.jsp page.

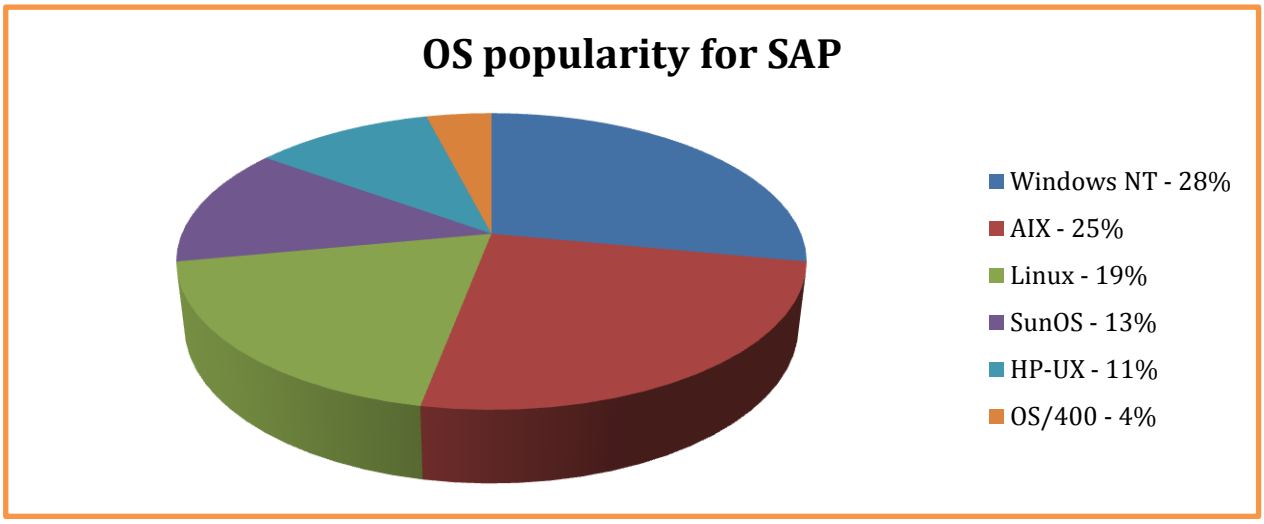
The detailed information about the major versions is presented below.



5.3. OS popularity for SAP

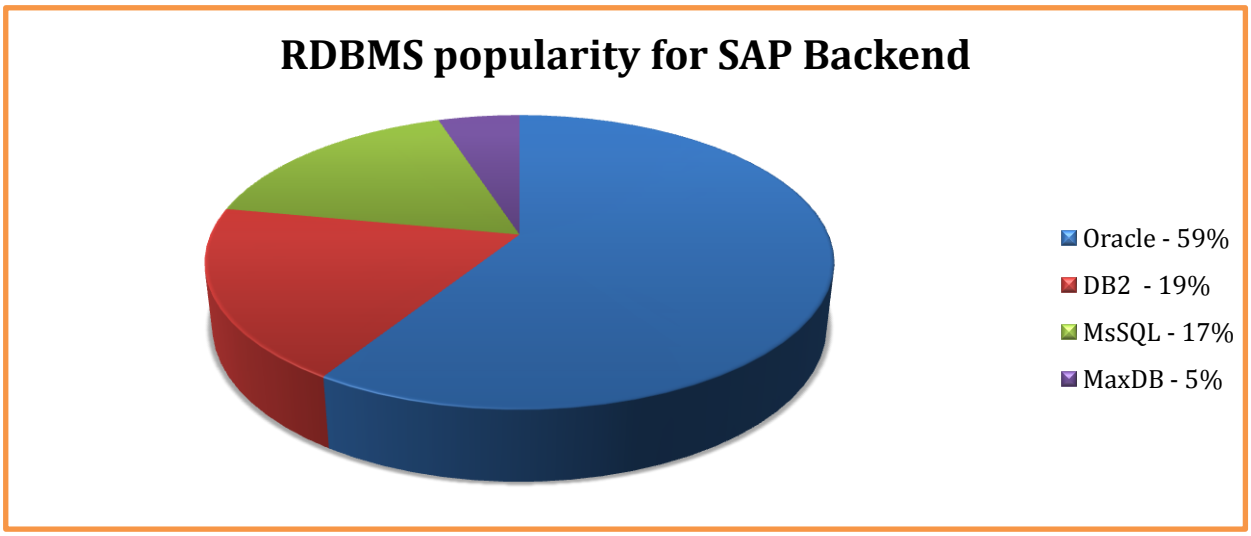
Using the /sap/public/info URL, it is possible to obtain information about OS versions for ABAP implementations. While analyzing the results that were gathered from Internet facing SAP systems, we found that the most popular OS is Windows NT (28%) and AIX (25%). According to our statistics from internal SAP assessments, *.NIX systems are more popular while Windows is more popular for Internet facing SAP systems.

The most popular OS for SAP are Windows NT (28%) and AIX (25%)



5.4. RDBMS popularity for SAP Backend

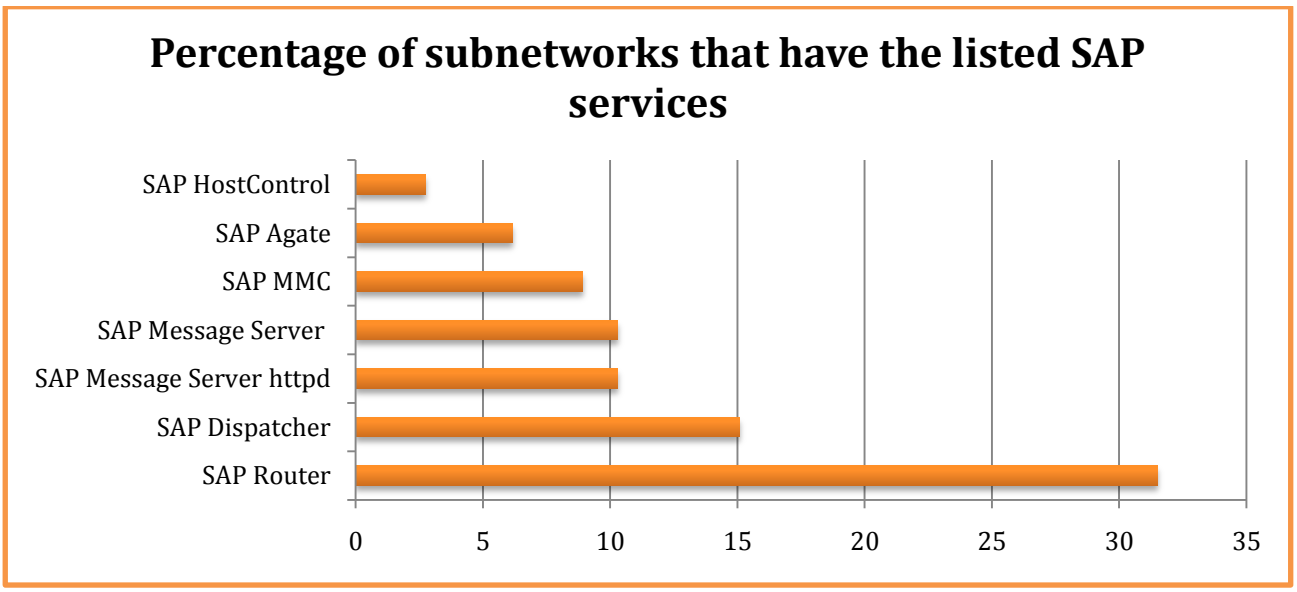
The most popular RDBMS used as a backend for SAP is still Oracle – 59%. Other RDBMS systems are listed below.



It should be mentioned that Oracle RDBMS installed with SAP is vulnerable to a very dangerous attack, where authentication is bypassed and an unauthorized attacker obtains direct access to the database system without any authorizations because of the improper use of REMOTE_OS_AUTHENT parameter. It is a very old bug first published in 2002 but still active [29].

6. Critical services on the Internet

Apart from the web interfaces that should be enabled on the Internet because of various business needs, such as SAP Portal, SAP SRM or SAP CRM solutions, there are some services that should not be available externally at all. Not only do they bring a potential risk but they have real vulnerabilities and misconfigurations which are well-known and well-described in public resources. Of course it is not the full list of critical SAP services, just the most popular ones. The scan was performed across 1000 sub networks of companies that use SAP worldwide. In the graph you can see the percentage of companies where SAP services, other than web based, were open for remote connection.



As you can see, SAP Router is the most popular service and it is normal because its business purpose is to be open for external connections. But what about other services? They should not be available from the Internet but they are. And the number of them is not as small as we thought before starting this project.

Services like SAP Dispatcher, SAP Message server, SAP HostControl and more, presented on slides, should not be open for connecting through the Internet

6.1. WebRFC service as part of NetWeaver ABAP

WebRFC is a web service which is available by default in the SAP NetWeaver ABAP platform. It allows executing dangerous RFC functions using HTTP requests to the NetWeaver ABAP port and URL – /sap/bs/web/rfc. Among those functions, there are several critical ones, such as:

- Read data from SAP tables
- Create SAP users
- Execute OS commands

- Make financial transactions etc.

By default, any user can have access to this interface and execute the RFC_PING command by sending an XML packet. Other functions require additional authorizations. So there are 2 main risks:

- If there is a default username and password in the system, an attacker can execute numerous dangerous RFC functions because default users have dangerous rights.
- If a remote attacker obtains any existing user credentials, he can execute a denial of service attack on the server by sending the RFC_PING request with malformed XML packet [30], [31].

It was found that 40% of ABAP systems on the Internet have the WebRFC service enabled.

While we did not check if those systems had default passwords, according to different statistics obtained from our research and the research of our colleagues, about 95% of systems have at least 1 default user account.

6.2. CTC service as part of NetWeaver J2EE

CTC or ConfigTool is a web service which is installed by default on the NetWeaver J2EE engine. It allows controlling the J2EE engine remotely. This is a web service which can be found by Google and it often exists on SAP Portals. It is possible to execute such functions as:

- Create users
- Assign a role to a user
- Execute OS commands
- Remotely turn J2EE Engine on and off

The researchers from ERPScan have presented a vulnerability [9] in this service which is called Verb Tampering. It allows bypassing authorization checks for remote access to CTC service. It means that anybody can remotely obtain full unauthorized access to all business-critical data located in the J2EE engine.

It was found that 61% of J2EE systems on the Internet have the CTC service enabled.

While we did not scan those systems to find if they were vulnerable or not but, according to our statistics from penetration tests, about 50% of them are still vulnerable.

6.3. SAP Message Server HTTP

SAP Message Server HTTP is an HTTP port of SAP Message Server service which allows balancing the load on SAP Application Servers. Usually this service is only available inside the company but some implementations have been found that have external IP addresses, which is typically not needed for business processes and can lead to critical actions. By default, the server is installed on the 81NN port where NN is the system number [32]. One of the issues of SAP Message Server HTTP is a possibility to get the values of the configuration parameters of SAP system remotely without authentication. It can be used for future attacks.

During a sampling scan of 1000 sub networks which are assigned to companies that use SAP, 98 Message Server HTTP systems were found to be available.

Approximately every 10th company is vulnerable to unauthorized gathering of system parameters remotely from the Internet and most of them are located in China (55%) and India (20%)

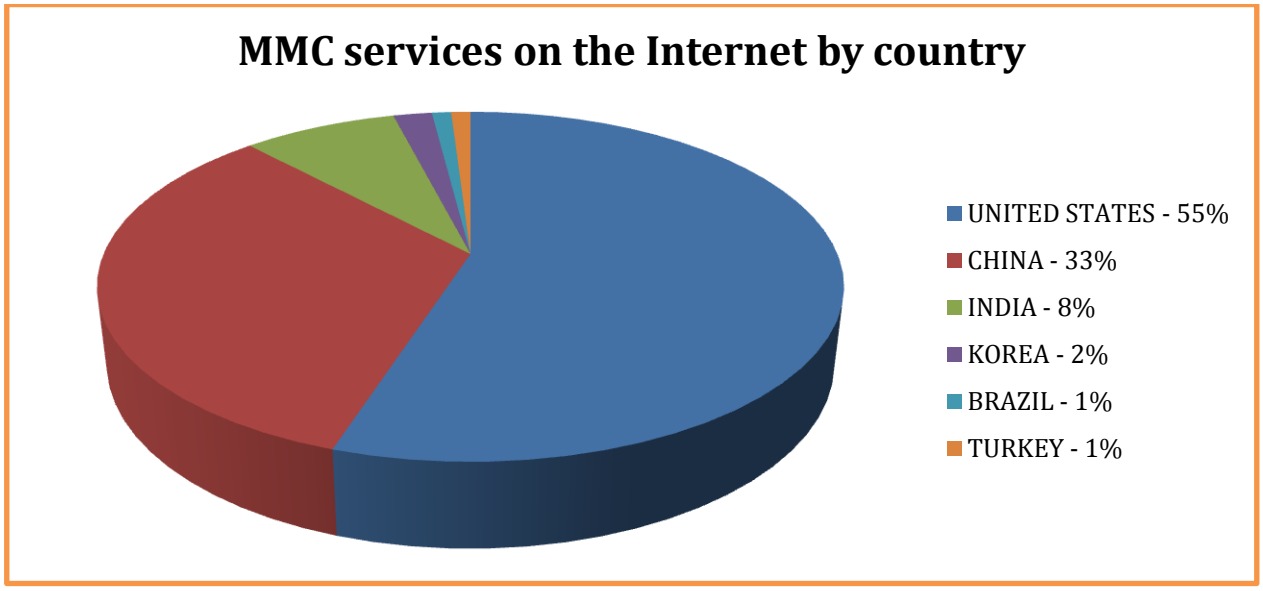
6.4. SAP Management console

SAP HostControl is a service which allows remote control of SAP systems. The main functions are remote start and stop and they require the knowledge of username and password. Apart from the functions which require authentication, there are some functions that can be used remotely without authentication. Most of them allow reading different logs and traces and sometimes system parameters. Those issues were well-covered by Chris John Riley, an independent researcher [33].

A more prevalent danger that ERPScan researchers have found is the possibility to find information about JSESSIONID in the log files [10]. JSESSIONID is an identification by which HTTP sessions are controlled. One of the possible attacks is to insert this JSESSIONID into a browser cookie and get unauthorized access to a user's session.

During the same scan as in the previous tests, it was found that 9% of subnetworks have Management console services open. 548 of them were found in total.

Approximately every 11th company is vulnerable to the attacks which allow obtaining log files or system parameters remotely.



6.5. Sap Dispatcher service

SAP Dispatcher is the main service for SAP client-server communications. It allows connecting to the SAP NetWeaver using the SAP GUI application through DIAG protocol. SAP Dispatcher port should not be available from the Internet directly and even in the internal network only appropriate users or user networks must have access*. Keep in mind that we are talking about Dispatcher not WEB Dispatcher which of course should be available from the Internet.*

Nevertheless, during a brief scan of 1000 subnetworks, we found 832 SAP Dispatcher services available on the Internet in 15% of networks.

Every 6th company is vulnerable to DOS attacks and unauthorized access with default passwords in SAP Dispatcher.

Why it is dangerous?

First of all, this service allows direct connection to a SAP system using SAP GUI where all that an attacker needs is a valid username and password. There are numerous default passwords in SAP and, according to our statistics of penetration testing; about 95% of systems have default credentials.

Another problem, which was found some time ago by Core Security, is that the SAP Dispatcher service has multiple buffer overflow vulnerabilities that can lead to the denial of service attack and one of them also allows code execution [34]. The exploit code was published on May 9 and an unauthorized cybercriminal can exploit it without any rights. The good news is that this vulnerability only works when DIAG trace is set to level 2 or 3 which is not a default value but a possible one anyway. There can be other issues in this service so it must be disabled for external access.

7. Conclusion

We can conclude that the interest to SAP platform security has been growing exponentially. Taking into account the growing number of vulnerabilities and vast availability of SAP systems on the Internet, we predict that SAP systems can become a target not only for direct attacks (for example APT) but also for mass exploitation using worms targeting one or more vulnerabilities. We are working closely with the SAP Security Response Team on discovering and patching security issues and also SAP publishing secure recommendations and guidelines showing administrators how to protect from most popular threats. Now the main mission lies with administrators who should enforce security of their SAP systems by using guidelines, secure configuration, patch management, code review and continuous monitoring.

About OWASP-EAS

The OWASP Enterprise Application Security Project (OWASP-EAS) exists to provide guidance to people involved in the procurement, design, implementation or sign-off of large scale (i.e. “Enterprise”) applications.

Project mission

The security of enterprise applications is one of the major topics in the field of information security because those applications control money and resources and every incident of security violation can result in significant financial losses. The purpose of this project is to alert users to the enterprise application security problems and create guidelines and tools for enterprise application security assessment.

Our primary goals are:

1 To alert users to enterprise application security by releasing annual statistics of enterprise business application vulnerabilities and security trends.

2 To help companies to begin assessment of enterprise applications

3 To help software vendors improve security of their solutions

4 To develop free tools for enterprise business applications assessment

Links and future reading

1. http://erpscan.com – the website of company focused on SAP Security solutions development.
2. http://sapscan.com – the website of project dedicated to global SAP port scanning
3. http://www.lasvegassun.com/news/2009/nov/06/managing-fraud-lesson-recession/
4. http://erpscan.com/publications/sap-security-attacking-sap-clients/
5. http://cansecwest.com/slides06/csw06-lord.ppt
6. http://erpscan.com/products/erpscan-pentesting-tool/
7. http://erpscan.com/products/erpscan-webxml-checker/
8. http://www.cybsec.com/EN/research/sapyto.php
9. http://erpscan.com/wp-content/uploads/2011/08/A-crushing-blow-at-the-heart-SAP-J2EE-engine_whitepaper.pdf
10. http://erpscan.com/wp-content/uploads/2012/06/Top-10-most-interesting-vulnerabilities-and-attacks-in-SAP-2012-InfoSecurity-Kuwait.pdf
11. http://scn.sap.com/docs/DOC-8218 – Acknowledgments to Security Researchers
12. http://cve.mitre.org – Common Vulnerabilities and Exposures
13. http://securityfocus.com – Vulnerability Database
14. http://exploit-db.com – Exploit Database by Offensive Security
15. http://erpscan.com/advisories/dsecrg-11-041-sap-netweaver-authentication-bypass-verb-tampering/
16. http://virtualforge.com/tl_files/Theme/whitepapers/201106_SAP_Security_Recommendations_Protecting_JAVA_ABAP.pdf
17. http://help.sap.com/saphelp_nw70ehp2/helpdata/en/bb/f2b9d88ba4e8459e5a69cb513597ec/frameset.htm
18. http://virtualforge.com/tl_files/Theme/whitepapers/BlackHat_EU_2011_Wiegenstein_The_ABAP_Underverse-WP.pdf
19. http://erpscan.ru/advisories/dsecrg-11-039-sap-netweaver-th_grep-module-code-injection-vulnerability-new/
20. http://www.onapsis.com/resources/get.php?resid=adv_onapsis-2011-002
21. http://virtualforge.com/tl_files/Theme/Presentations/HITB2011.pdf
22. http://www.taddong.com/docs/BlackHat_EU_2011_Siles_SAP_Session-Slides.pdf
23. http://www.sensepost.com/cms/resources/labs/tools/poc/sapcap/44con_2011_release.pdf
24. http://www.cio.com/article/216940/The_ERP_Security_Challenge
25. http://erpscan.com/press-center/blog/sap-infrastructure-security-internals-google-and-shodan-hacking-for-sap/
26. http://erpscan.com/press-center/blog/sap-application-server-security-essentials-default-passwords/
27. http://erpscan.com/advisories/dsecrg-11-023-sap-netweaver-sld-information-disclosure/
28. http://erpscan.com/advisories/dsecrg-11-027-netweaver-bcb-%E2%80%93-missing-authorization-information-disclosure/
29. http://www.lan-ks.de/~jochen/sap-r3/ora-hack-en.html

30. http://erpscan.com/advisories/dsecrg-11-029-sap-netweaver-soap-rfc-%E2%80%93-denial-of-service-integer-overflow/
31. http://erpscan.com/advisories/dsecrg-10-005-sap-netweaver-xrfc-%E2%80%94-stack-overflow/
32. http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/4e515a43-0e01-0010-2da1-9bcc452c280b?QuickLink=index&overridelayout=true&42472931642836
33. http://www.slideshare.net/ChrisJohnRiley/sap-insecurity-scrubbing-sap-clean-with-soap
34. http://blog.coresecurity.com/2012/05/09/core-labs-discovery-of-six-vulnerabilities-within-sap-netweaver/

Our contacts

E-mail: a.polyakov@erpscan.com

Web: https://www.owasp.org/index.php/OWASP_Enterprise_Application_Security_Project