ERPScan

ANALYSIS OF 3000 VULNERABILITIES IN SAP

by

ERPScan Research Team

2014

Disclaimer

The partnership agreement and relationship between ERPScan and SAP prevents us from publishing the detailed information about vulnerabilities before SAP releases a patch. This review will only include the details of those vulnerabilities that we have the right to publish as of the release date. However, additional examples of exploitation that prove the existence of the vulnerabilities are available in conference demos as well as at ERPScan.com [1].

Our SAP security surveys and research in other areas of SAP security do not end with this whitepaper. You can find the latest updates about the statistics of SAP services found on the Internet and other endeavors of the EAS-SEC project [2] at SAPScan.com [3].

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

This document or any part of it cannot be reproduced in whole or in part without prior written permission of ERPScan. SAP AG is neither the author nor the publisher of this whitepaper and is not responsible for its content. ERPScan is not responsible for any damage that can be incurred by attempting to test the vulnerabilities described here. This publication contains references to SAP AG products. SAP NetWeaver and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany.

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 of the 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. Global fraud loss is estimated at more than $3.5 trillion for 2010–2012[5]. Thus, a typical entity loses 5% of annual revenue to fraud. The average value for 4 years is 6%. That is why we decided to increase awareness in this area.

Losses to internal fraud constituted 6% 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 8 years, SAP security experts have spoken a great deal about various attacks on SAP from the RFC interface, SAProuter, SAP WEB and SAP GUI client workstations [6]. Interest in the topic has been growing exponentially: in 2006, there was 1 report [7]on SAP at a technical conference dedicated to hacking and security, whereas in 2013 there were more than 30 of them already.

According to the statistics of vulnerabilities found in SAP applications, there were more than 100 vulnerabilities patched in SAP products in 2009, while it grew to more than 3000 in May 2014.

Many SAP vulnerabilities allow an unauthorized user to gain access to all critical business data, so it is necessary to consider the main attack vectors and the ways to secure those highly critical systems

2. Brief results

Here you can find highlights of our review:

- ***"Percentage of vulnerabilities in SAP is much higher that people usually think"*** number of vulnerabilities closed by SAP is more than 3000 which is equals to about 5% of all vulnerabilities ever published on the Internet.

- ***"Interest in SAP security is growing exponentially"*** number of vulnerabilities found by 3rd parties comparing to vulnerabilities patched by SAP has grown from about 10% in late 2000s to 60-70% in recent monthly updates.

- ***"SAP is making good steps in SDLC"*** - number of vulnerabilities in SAP per month has decreased approximately 2 times comparing to the high peak in 2010.

- ***"Number of companies which find issues in SAP is growing"*** – almost 60 companies have acknowledges from SAP by June 2014. The number is growing every year in about 50%.

- ***"Interest in hacking of NEW SAP products is growing"*** - number of issues found in new SAP products, like SAP HANA, is growing faster than in others, although there are about 10 issues in total.

- ***"What is popular with traditional security is not always popular with SAP security"*** - memory corruption vulnerabilities are 7 times less popular in SAP than in general types of products.

- ***"SAP is a very complicated system, and a significant part of security measures lies on the shoulders of the administrators"*** - configuration issues in SAP are 5 times more popular than in general types of products.

The interest in SAP platform security has been growing exponentially, and not only among whitehats. SAP systems can become a target both for direct attacks (e. g. APT) and for mass exploitation because a range of simply exploitable and widely installed services is accessible from the Internet.

Analysis of 3000 vulnerabilities in SAP

From cvedetails.com, a website which calculate most vulnerable vendors by the number of CVE's SAP is on the 37th place in the complete list of vendors, but not all SAP issues have CVE's. SAP itself don't publish them and external researchers also do it from time to time. However if we count by the number of public advisories (there are about 500 of them) SAP is on the 15th place. What is more interesting, if we count by the total number of closed vulnerabilities (more than 3000 security notes). SAP will be on the second place after the Microsoft, but it is not proper comparison, at least because Microsoft probably close much more issues internally

While the number of vulnerabilities closed by SAP Security Notes (small patches) per year is decreasing, SAP moves a lot of vulnerabilities to Service Packs, leaving in security notes only highly critical issues and the issues which were found by external researchers. So, in previous years, only about 10% of monthly published vulnerabilities were found by external researchers but up to 60-70% in more recent updates. At the same time, the total number of SAP security patches per year is decreasing.

Different SAP products have different amount of vulnerabilities found per year. For some new SAP platforms, such as HANA, the percentage of issues is growing each year, whereas for JAVA platforms the percentage of issues is roughly the same each year. At the same time, the amount of issues found in the old platforms, such as ABAP, is decreasing a bit, and the number of vulnerabilities found in client applications, comparing to the peak in 2010 when we started to explore them, is going down significantly.

While typical issues have, more or less, the same results, we have two areas where the statistics go different. First of all memory corruption vulnerabilities such as buffer overflow - the most popular vulnerability in the world (14% of all issues) - constitute only 2% in SAP, and only 1% of them is actually remotely exploitable, and even those are mostly on client applications. The reason is simple. Memory corruption issues are hard to exploit in SAP. That is why we always say in our workshops and trainings that you need payloads for different versions and platforms. But there always remains a slight chance of something going wrong. However, for pentesters and especially for cybercriminals, those issues are not interesting because issues related to configuration, access control, or authentication are much easier to use both for pentest and for fraud.

Secondly, the number of issues related to configuration is about 11% of SAP issues, while in general those issues only constitute about 2%. This result is quite predictable for people who have been in SAP security for a long time. They know that the biggest problem is the complexity and customization of SAP solutions. SAP has thousands of different configuration tweaks in multiple platforms, and they make a real difference. Unfortunately, those configuration issues are not so easy to patch because they affect business processes. At the very least, you have to reboot the system to reconfigure it. For example, to close a vulnerability in the authentication protocol of the SAP Software Deployment service, the new version of client and server software have to be installed, and it can sometimes be quite challenging. It is harder to monitor, check, and control than simply apply patches, which usually close only typical issues, such as XSS or Directory Traversal.

3. General vulnerability statistics

We took all information related to SAP Security notes to analyze it by different parameters such as year, criticality, type, affected platform or software component and also compare those parameters to figures related to all product vulnerabilities. Data about all existing vulnerabilities were taken from The SAP Support Portal [1], the annual report «SAP Security in Figures – a global survey 2013» [2] SourceFire's report «25 years of vulnerabilities: Past, Preset and future» [3], http://www.cvedetails.com/ [4] website and some other sources.

3.1. Number of SAP Security Notes

Every month on SAP Critical Patch Day (every second Tuesday), SAP releases one or more internal advisories called SAP Security Notes. 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. In 2007, the number of published notes began to grow exponentially having its peak in 2010. Later, the number of SAP security notes began to fall, but still remain on quite high value.

3013 SAP Security Notes have been published By 10'th June 2014

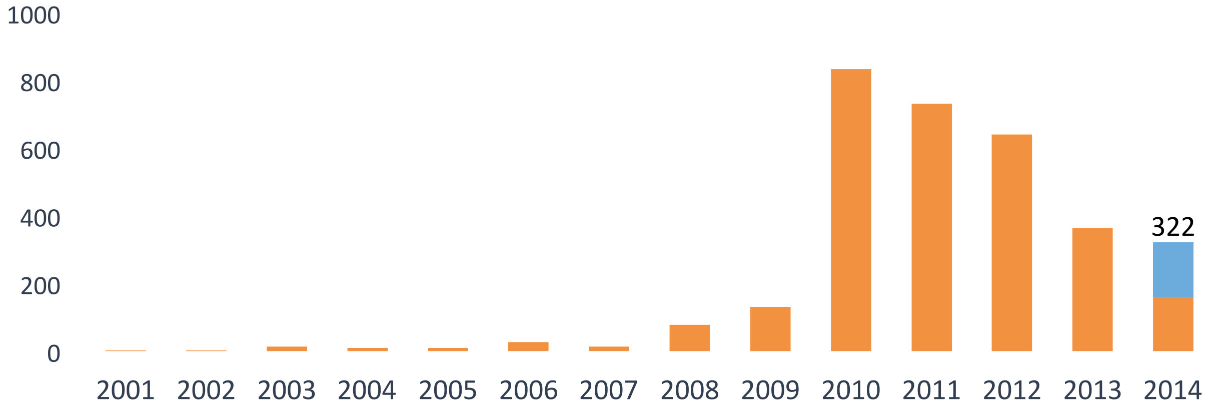

Figure 3.1-1. Number of Sap Security Notes per year: 2001-2014

Number of vulnerabilities closed by SAP is about 5% of all existing vulnerabilities

Analysis of 3000 vulnerabilities in SAP

In the beginning of 2013, when Sourcefire released report about vulnerabilities in 25 years, where a total of 54000 vulnerabilities were published, SAP had about 2600 vulnerabilities in their products. By the June 2014 according to cvedetails totally there are 62113 vulnerabilities in all products and 3013 in SAP so number of vulnerabilities closed by SAP equal to approximately 5% of all existing vulnerabilities in the world not taking into account that some SAP Security notes may close more than one vulnerability.

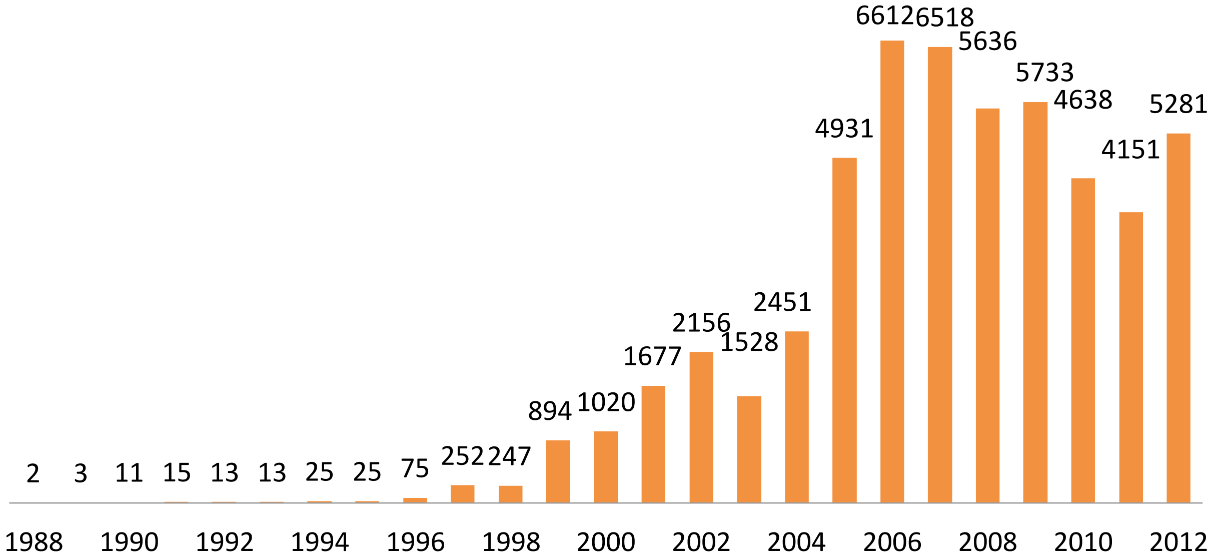

Figure 3.1–2 Number of public vulnerabilities in all products of all vendors per year

3.2. Comparison to other vendors

We took information about all published vulnerabilities by different vendors from sourcefire's report. Unfortunately we were unable to find information about SAP issues because of 2 things. First of all not every vulnerability patched by SAP can be found somewhere in public resources such as CVE because about 85% of SAP vulnerabilities are closed internally and information about them and patch are only available to SAP customers and partners. Even those 15% vulnerabilities that found by external researchers are not all assigned to CVE. Usually Product vendors coordinate with CVE and assign vulnerabilities such as Microsoft or Oracle do. However SAP do not coordinate with CVE. Most of the researchers don't do it as well, because it takes lots of time but don't give any visible benefits.

As a result, only about 160 SAP vulnerabilities have CVE, so if we look at the SAP's place in the list of top vulnerable vendors at cvedetails we will find it only on 37th place [7] However if we count by the number of public advisories (there are about 500 of them) SAP is on the 15th place. What is more interesting, if we count by the total number of closed vulnerabilities (3013 SAP Security Notes). SAP will be on the second place after the Microsoft, but it is not proper comparison, at least because Microsoft probably close much more issues internally.

Place	Vendor	Number of vulnerabilities
1	Microsoft	3392
2	Oracle	2259
3	Apple	2245
4	IBM	2041
5	Cisco	1048
6	SUN	1581
7	Mozilla	1318
8	Linux	1191
9	HP	1115
10	Google 1086	1086

Table 3.2. Vulnerabilities closed by different vendors by June 2014

3.3. SAP Security Notes sorted by criticality

SAP has now 4 different levels of criticality for published notes:

1. Hot News
2. Correction with high priority
3. Correction with medium priority
4. Correction with low priority

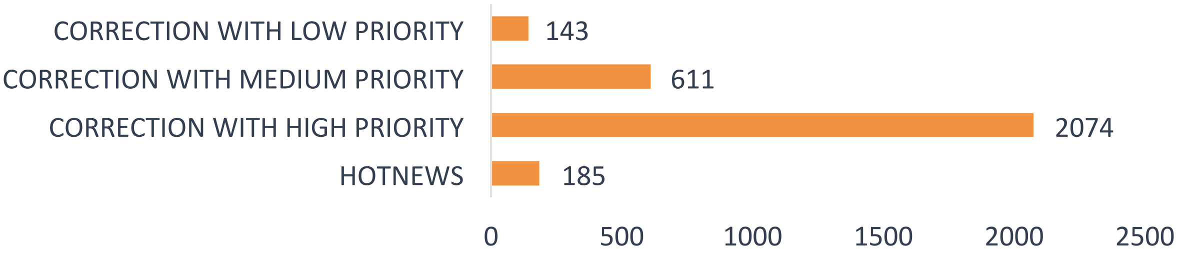

Figure 3.3-1. Number of Sap Security Notes, sorted by criticality level

Before November 2013 there was also 5th level - additional information.

In comparison with the total number of SAP Security Notes obtain the following percentages of each type of criticality:

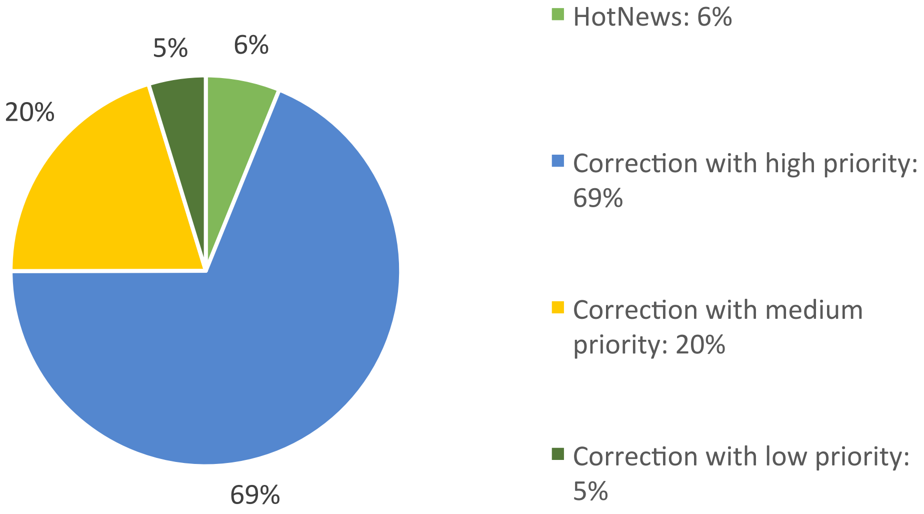

Figure 3.3-2. Number of Sap Security Notes, sorted by criticality level in percentage

Most of the 69 issues have HIGH priority,
which means that 69% of the published vulnerabilities must be corrected quickly

So we can trace the attitude is very important (sum of high priority and Hotnews priority) security update in relation to the total amount for the year:

3.4. SAP Security Notes by Type

All published SAP Security Notes were analyzed by vulnerability type. About 300 of vulnerabilities were assigned to configuration issues.

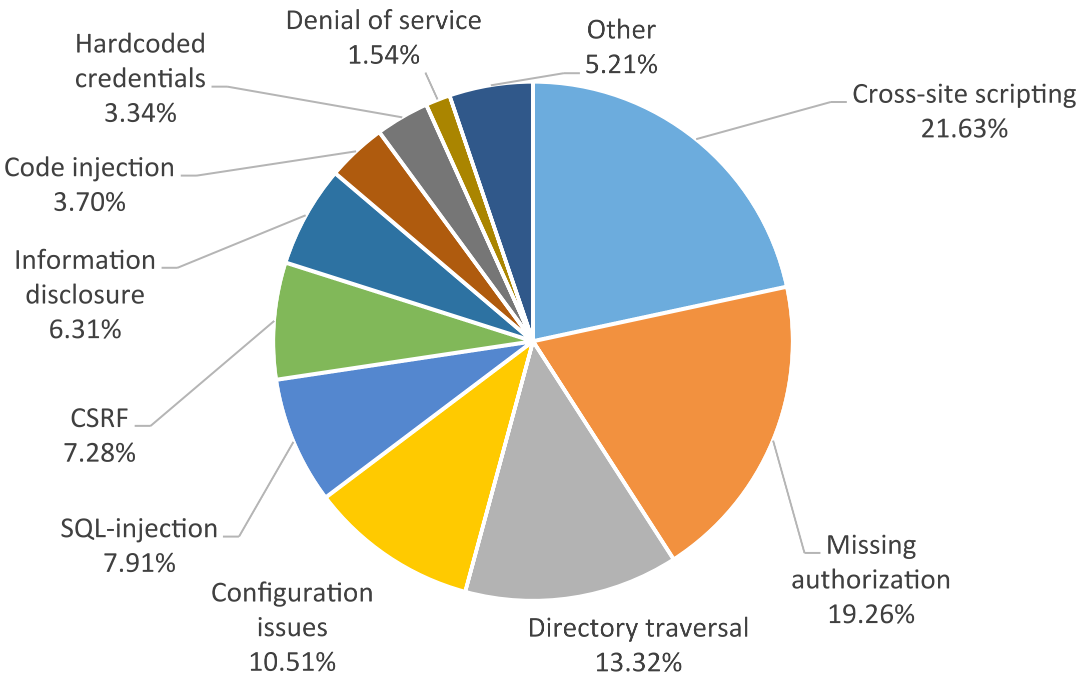

Figure 3.4-1 TOP-10 SAP Security Vulnerabilites, sorted by type

Vulnerabilites	proportion of total
Cross-site scripting	21,63
Missing authorization	19,26
Directory traversal	13,32
Configuration issues	10,51
SQL-injection	7,91
CSRF	7,28
Information disclosure	6,31
Code injection	3,70
Hardcoded credentials	3,33
Denial of service	1,53
Other	5,2

Table 4.1 TOP-10 SAP Security Vulnerabilities, sorted by type

About 5% of found vulnerabilities are not included in the top 10 because a lot of unique and unknown issues exist in SAP systems. Some of them are available in our presentation called “Top 10 most interesting SAP vulnerabilities and attacks” [11].

Analysis of 3000 vulnerabilities in SAP

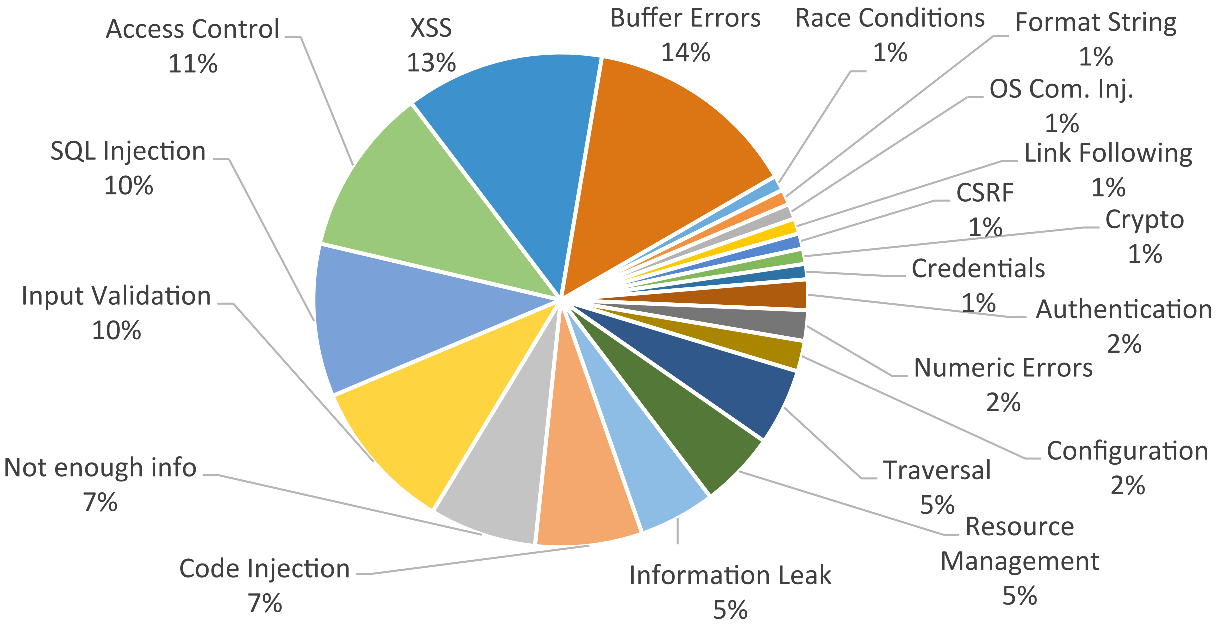

Figure 3.4-2 Security Vulnerabilities in all products of all vendors, sorted by type

In addition, we compared the SAP vulnerability lists for 2012 and 2013 and the OWASP Top10 to see if there are any differences between web-based issues and business application issues and if there are any changes.

Vulnerability type	Percent in SAP	Percent in world statistics	CWE-ID	Place in SANS TOP 25	Place in OWASP TOP 10
XSS	21,63	13%	CWE-79	4	3
Missing authorization	19,26	11% (Access Control)	CWE-862	6	7
Directory traversal	13,32	5%	CWE-22	13	4
Configuration issues	10,51	2%	N/A	N/A	5
SQL Injection	7,91	10%	CWE-89	1	1
CSRF	7,28	1%	CWE-352	12	8
Information disclosure	6,31	5% (Information leak)	CWE-200	N/A	6
Code injection	3,70	7%	CWE-94	N/A	1
Hardcoded credentials	3,33	1%	CWE-308	7	2
Buffer Overflows (RCE+DOS)	1,53	14%	CWE-120	3	N/A

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 [12]. In the figure, you can see the number of vulnerabilities that were found by external researchers since 2010.

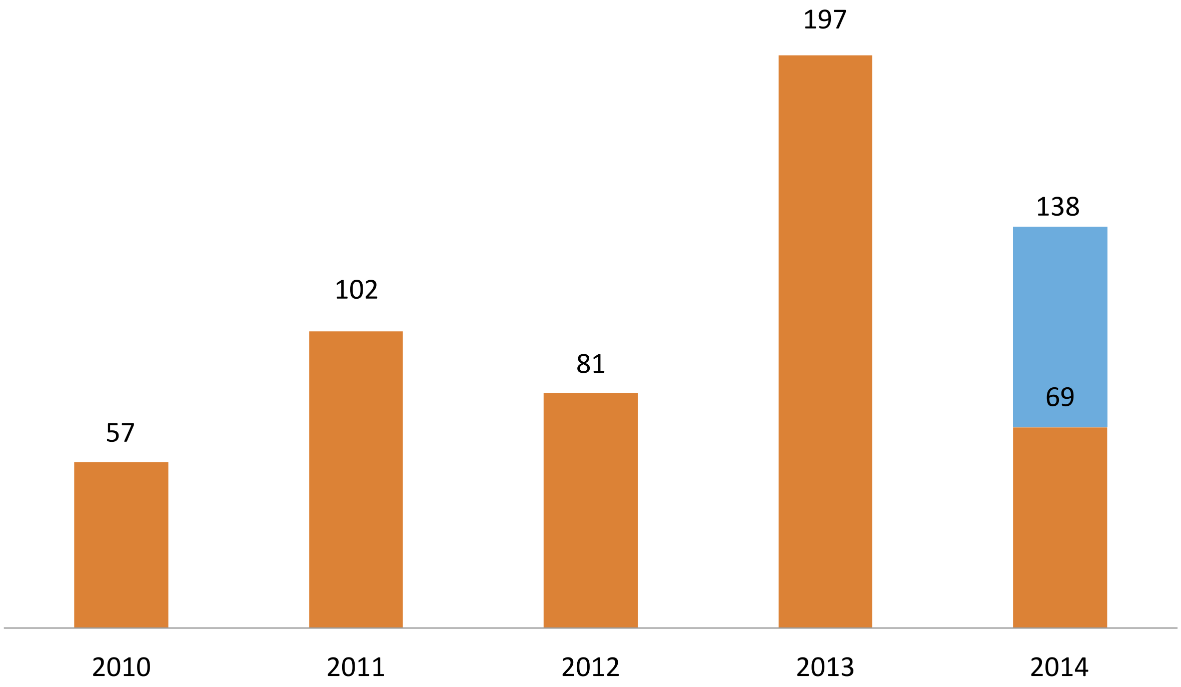

Figure 4-1. Number of vulnerabilities found by external researchers per year

In 2010, there were just 16 companies that had acknowledgements from SAP, but by the middle of 2014, we have counted 56 different companies and 3 researchers, which is almost 3 times more.

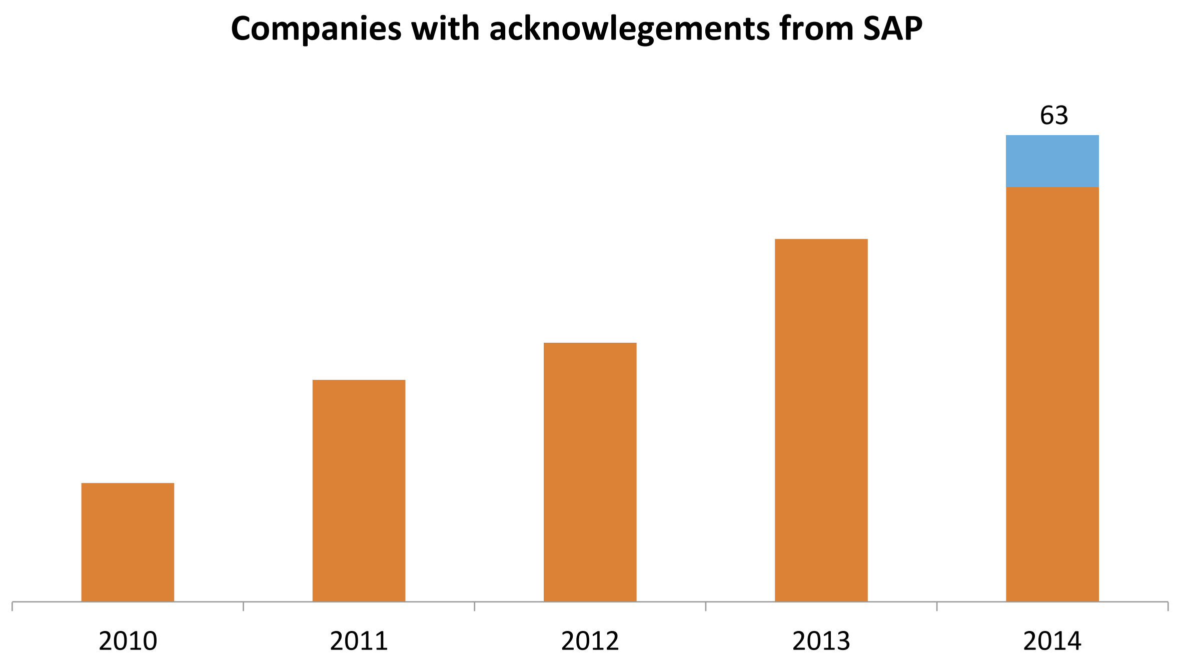

Figure 4–2 Number of companies acknowledged by SAP by year

External companies and researchers were acknowledged by SAP for helping to close more than 506 vulnerabilities in SAP products. Most companies were acknowledged just for only one vulnerability found with ERPScan being a company which found almost a quarter of all acknowledgements with near 100 of acknowledgements in total (much more than any other contributor).

The 80/20 rule works almost perfectly: 80 % of vulnerabilities were found by 15 % of companies

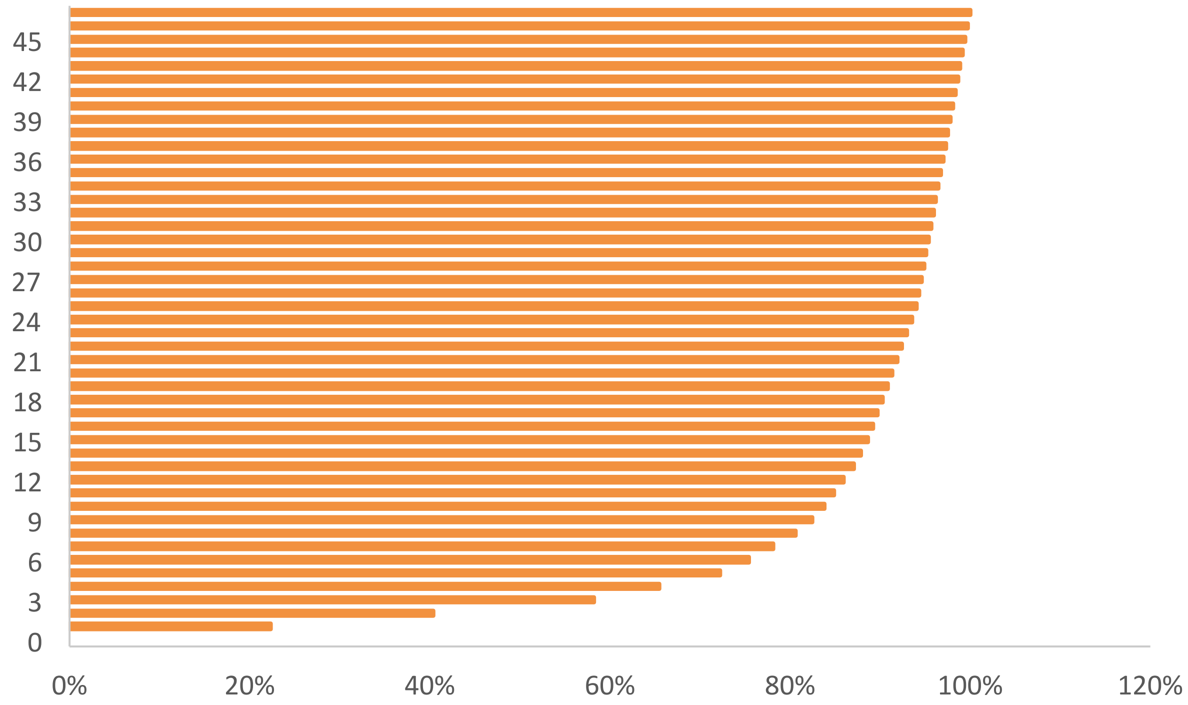

Figure 4–3 Percentage of acknowledgements vs. number of companies

The ratio of vulnerabilities found by external researchers versus vulnerabilities found by SAP internally is growing, as does the number of external researchers.

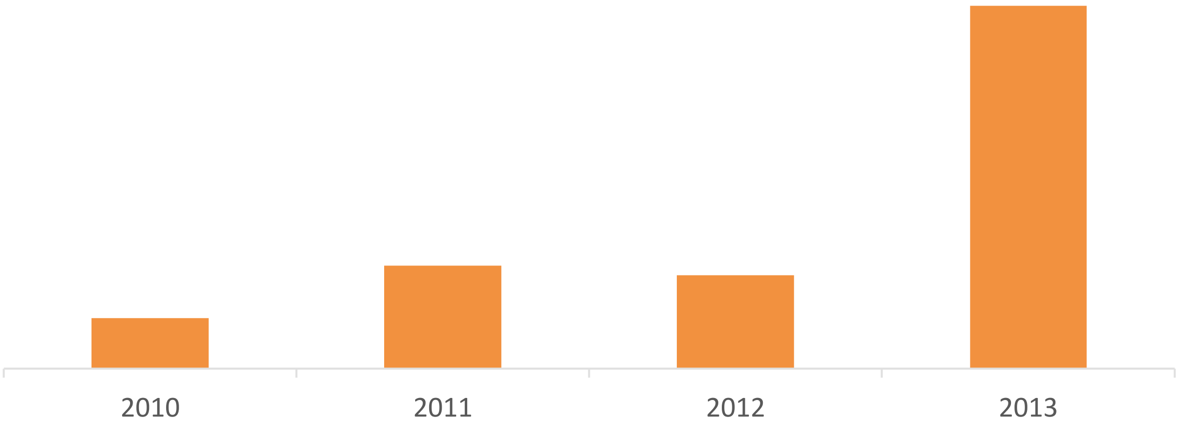

Figure 4–4 Percentage of acknowledgements to external researchers per year

What else can be archived from the relationship of SAP with external researchers? Recently, we have been receiving more and more responses from SAP PSRT to our reports about vulnerabilities, saying that they have already been patched before. This can be due to two reasons, and each of them is good news for SAP users. Firstly, SAP AG itself has significantly improved their internal SDLC and vulnerability research, so some issues were already found by SAP. Secondly, two different researchers sometimes get credits for the same issue, which means that the number of researchers is going to increase.

The record of bugs found by external researchers was cracked in January 2013: 76%

4.1. Amount of publicly available information

The most critical threat i can be from vulnerabilities found by 3'rd parties, the vulnerabilities which contain information about the methods of exploitation (detailed advisories, POC codes and working exploits) publicly available. Information was gathered from three most popular sources:

SAP SDN Acknowledgment page – List of acknowledges to different 3rd party researchers and partner companies**. 506 acknowledgements** (16.8% of all vulnerabilities) **were found here**.

Security Focus [13] – Detailed advisories, sometimes with POC code, can usually be found here. All the vulnerabilities published here have high probability of exploitation. **160 vulnerability advisories** (5.5% of all vulnerabilities) **were found here**.

Exploit-DB [16]– 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 50 exploits** (1.8% of all vulnerabilities) **were found here** (as of May'14).

In the figure 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.

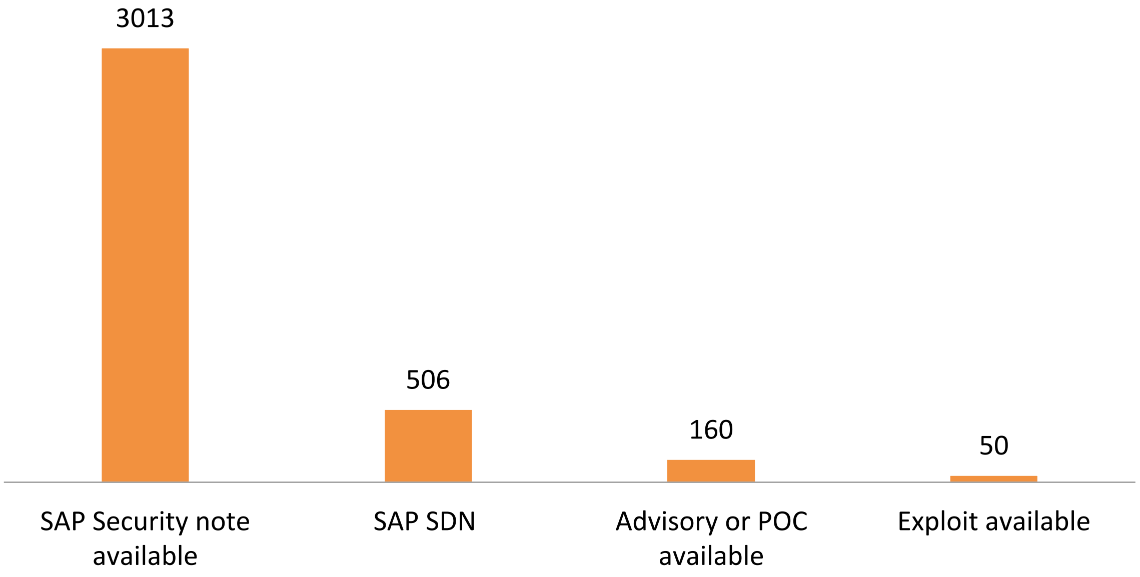

Figure 4.1-1 SAP vulnerabilities by probability and ease of exploitation, as of June 2014

5. Vulnerabilities sorted by engine

In the SAP systems there are several large popular platforms on which different systems are based. Among them there are 5 most popular areas:

- NetWeaver ABAP engine
- NetWeaver J2EE engine
- SAP HANA
- SAP Business Object
- Frontend applications

We do not consider the area in this publication, which came out little SAP Security Notes (including SAP Business One, MaxDB and others). We consider them as a separate type, buyout composes a small percentage of all the Notes. Moreover, we want to note that some of the notes are double stack. They fix bugs (or contain recommendations) for two components (either J2EE and ABAB). Sometimes it is not 100% clear which component is affected by note, so results may vary in about 1% but the trend stays clear anyway.

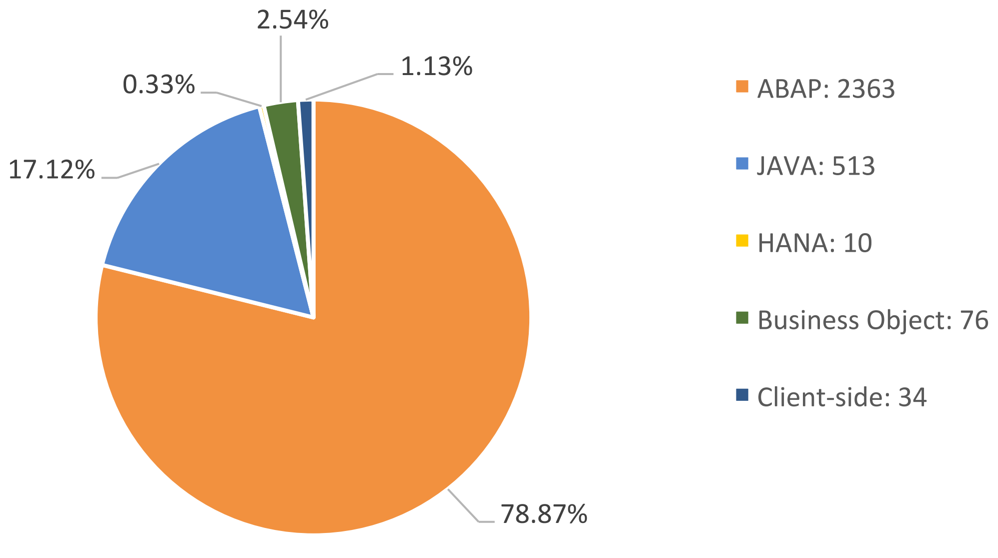

Figure 5.1. SAP Security Notes sorted by stacks

5.1. NetWeaver ABAP engine

Here we collect vulnerabilities in all products, which are based on SAP NetWeaver ABAP engine. Therefore, we include here Business applications like SAP ECC, HR, PLM, SRM and Industry Solutions as well as standalone applications, like SAP Router, SAP webdispatcher, SAP Enqueue server, SAP ITS, SAP IGS and some others.

As you may see, most popular vulnerabilities in ABAP engine are related to Missing Authorization checks and improper input filtration in ABAP programs. Absolute number of issues in ABAP engine is decreasing as well as an overall number of SAP Issues but relative number of issues in ABAP engine comparing to other engines is almost the same during latest 5 years.

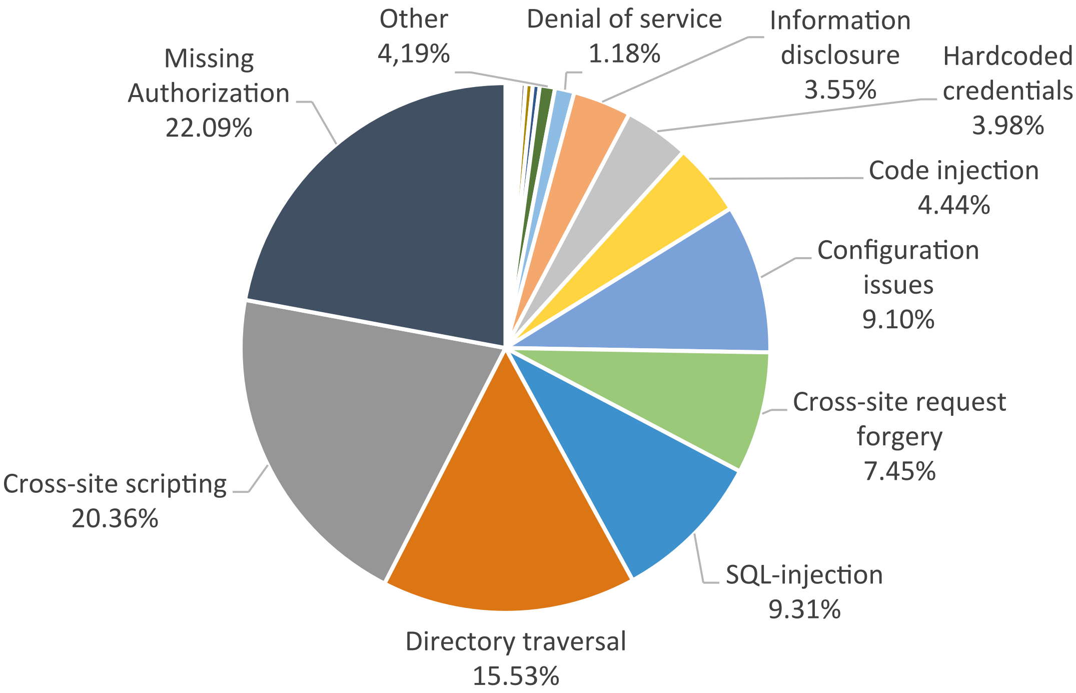

Figure 5.1-1 SAP Security Notes sorted by type in SAP NetWeaver ABAP engine

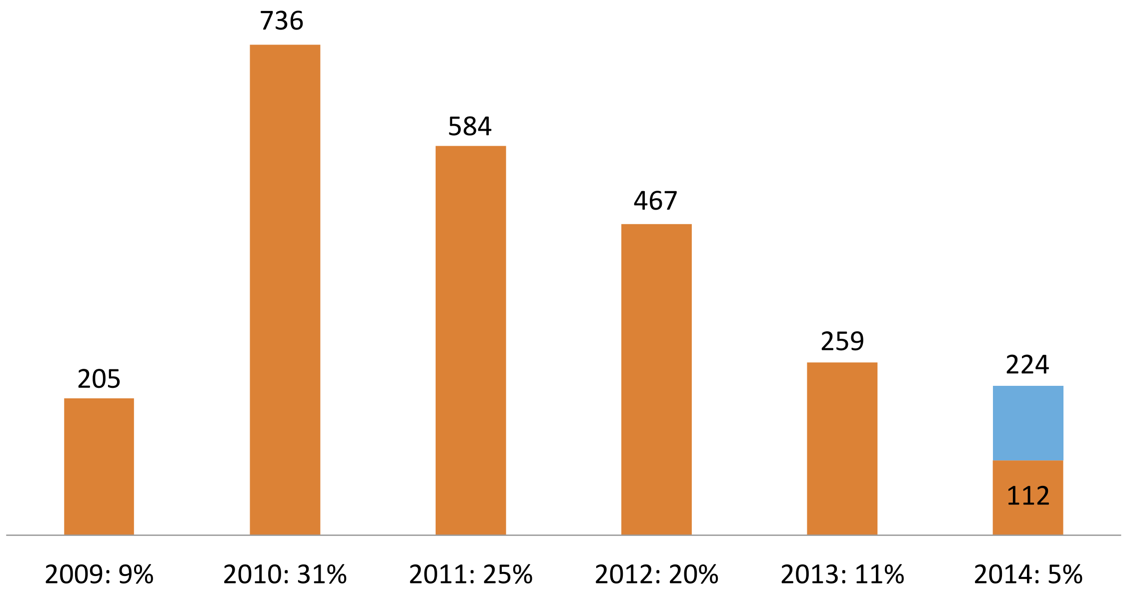

Figure 5.1-2 SAP Security Notes sorted by years in SAP NetWeaver ABAP engine

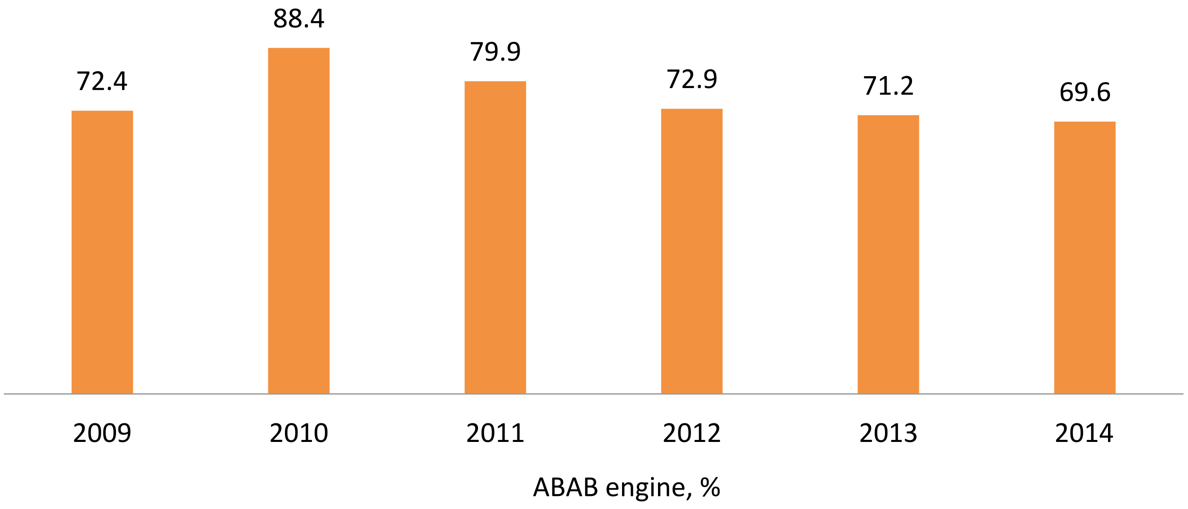

Figure 5.1-3 SAP Security Notes in SAP NetWeaver ABAP engine compared to all security notes by year

5.2. NetWeaver J2EE engine

All products, based on SAP NetWeaver J2EE Engine. Business applications like SAP Portal, SAP NetWeaver Developer Studio, SAP PI, Parts of SAP Solution Manager and other J2EE based components and products.

As you may see, most popular vulnerability in J2EE engine is XSS More than every forth vulnerability in J2EE engine is XSS. Taking into account that J2EE engine is a platform for SAP Portal, which is usually available on internet this issue may have, high risk.

Analysis of 3000 vulnerabilities in SAP

Absolute number of issues in J2EE engine begin to decrease in but relative number of issues in J2EE engine comparing to other engines is quite unpredicted, so it is not possible to say how it will look in next years and what are the current tendencies

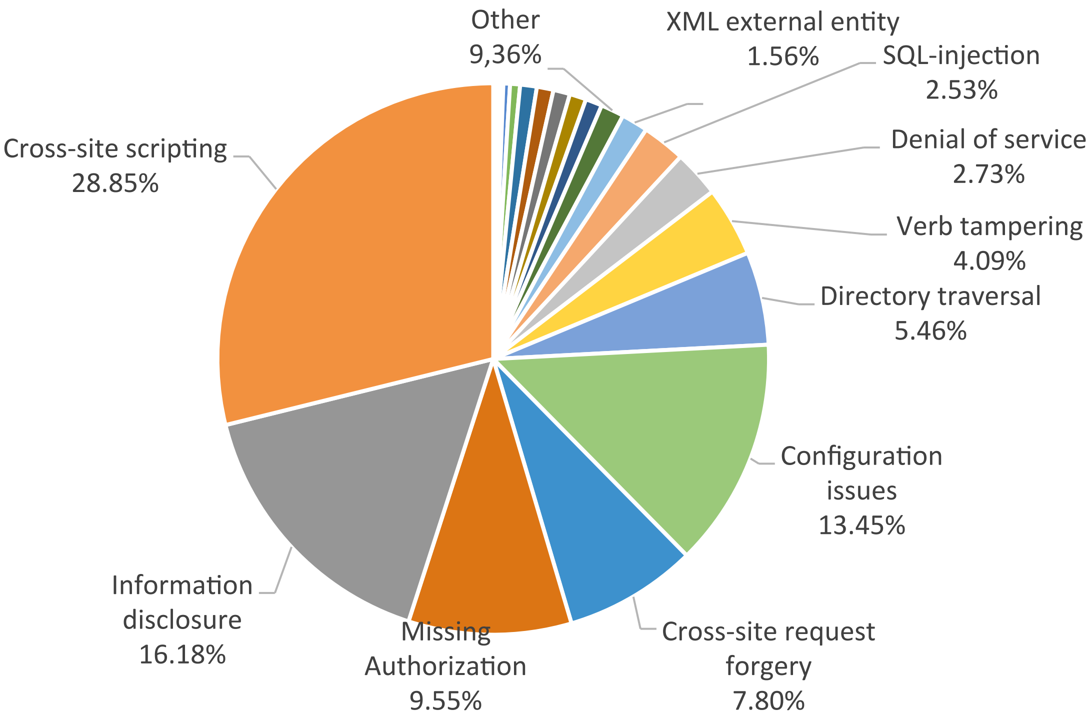

Figure 5.2-1 SAP Security Notes sorted by type in NetWeaver J2EE engine

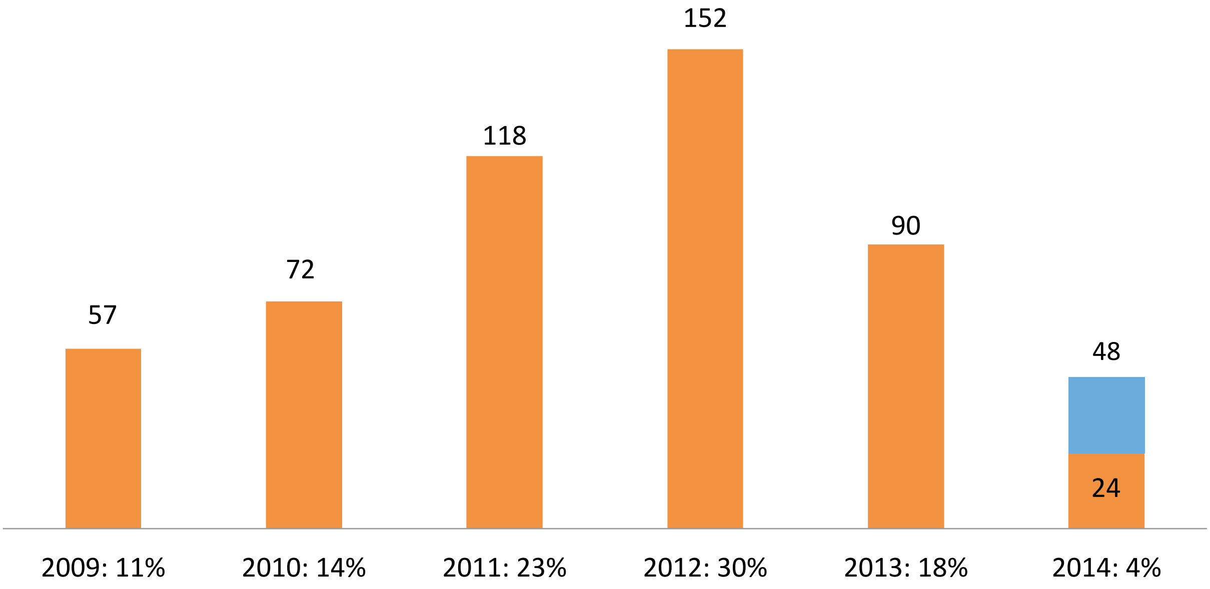

Figure 5.2-2 SAP Security Notes sorted by years in NetWeaver J2EE engine

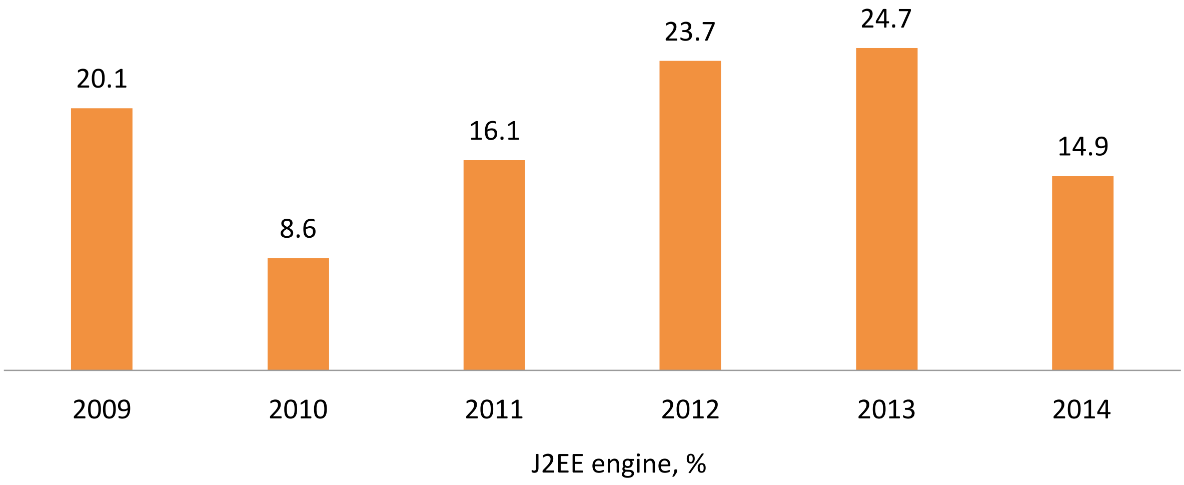

Figure 5.2-3 SAP Security Notes in NetWeaver J2EE engine compared to all security notes by year

5.3. SAP HANA

We consider all products, based on SAP HANA platform, including SAP HANA Database and SAP HANA XS Application server, and less popular components. This platform is a newest, so, not so much issues exist comparing to other platforms but the number of issues is significantly increasing and will increase much faster in future.

As you may see, most popular vulnerability in HANA is configuration issue, but honestly there were only 10 issues closed in SAP HANA so, it is not right time to make conclusions but one thing we know for sure, there will be much more issues in this platform in near future as this is quite popular platform.

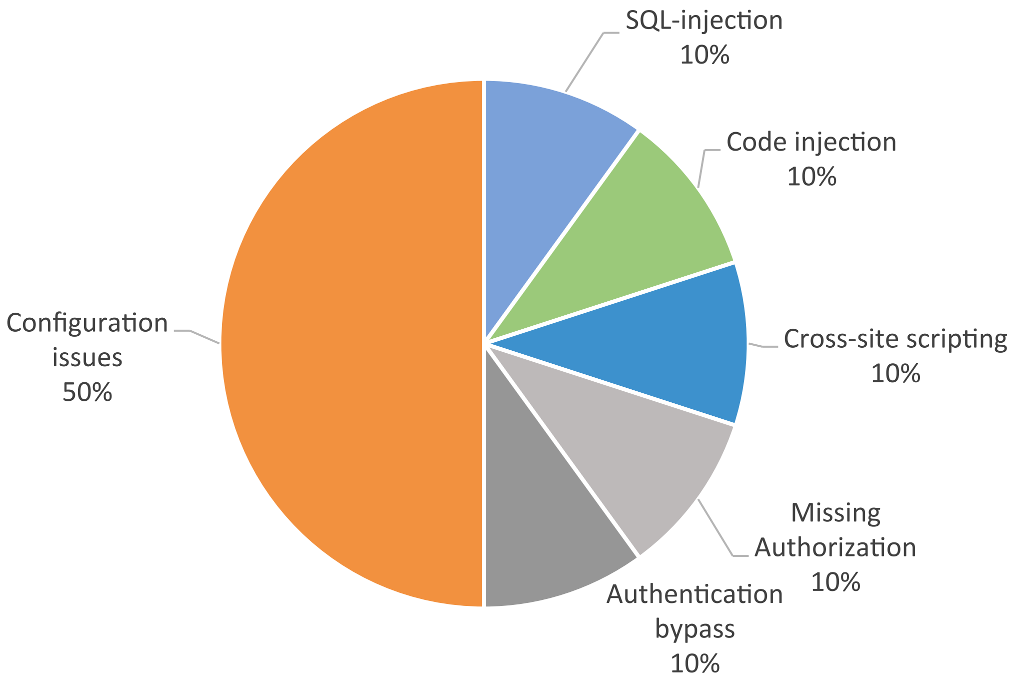

Figure 5.3-1 SAP Security Notes sorted by type in SAP HANA

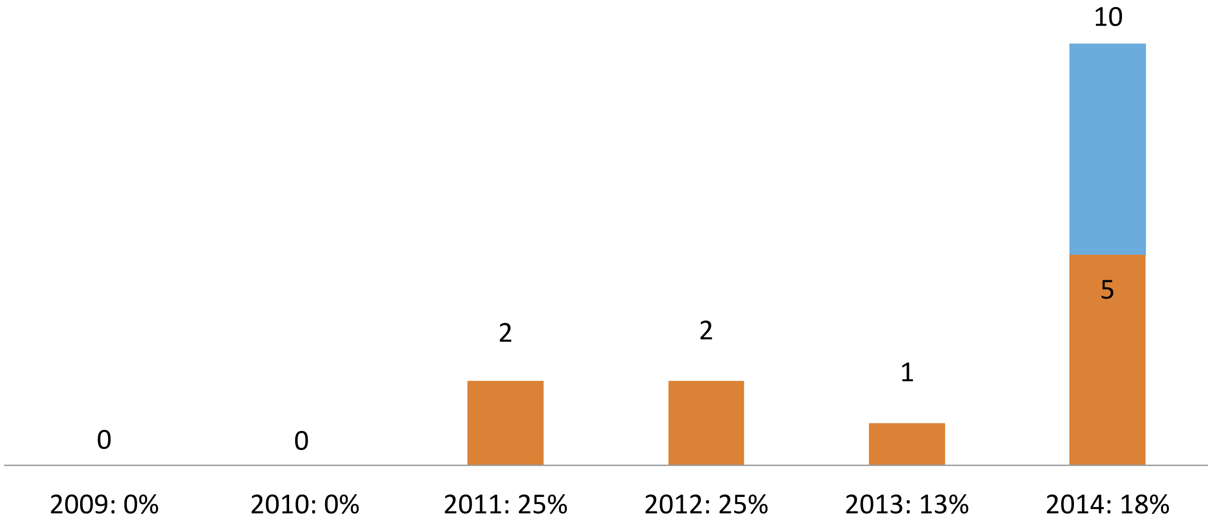

Figure 5.3-2 SAP Security Notes sorted by years in SAP HANA

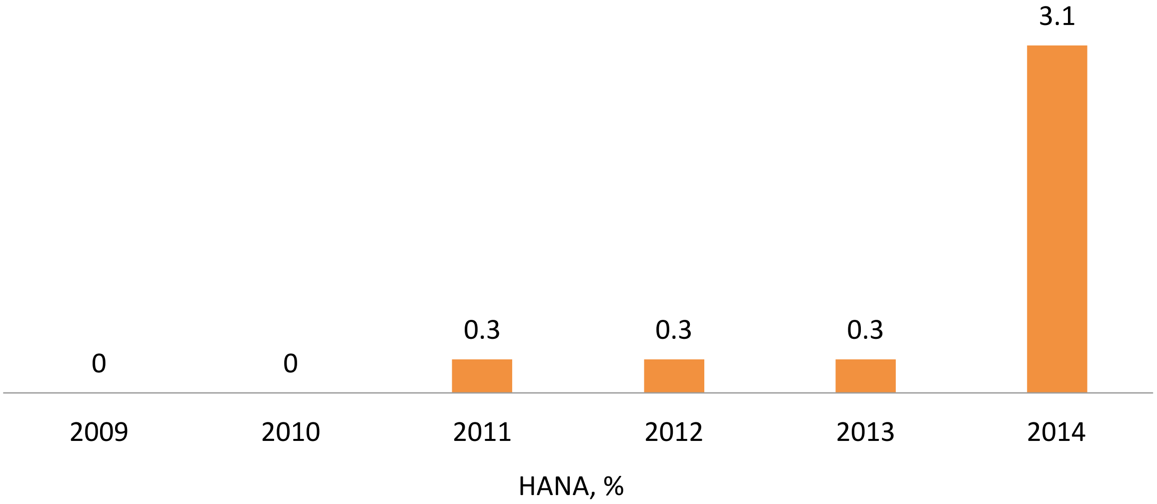

Figure 5.3-3 SAP Security Notes in SAP HANA compared to all security notes by year

5.4. SAP Business Objects

Here we consider all products based on SAP BusinessObjects engine. Business applications like SAP BI and fermer BusinessObjects products like BusinessObjects XI , Xcelsius, Data Services, Data Integrator and BusinessObjects Edge BI.

As you may see, most popular vulnerabilities in BusinessObjects engine are related to improper input filtration (XSS) and configuration issues. Absolute number of issues in BusinessObjects engine is going to increase as well as relative number of issues in BusinessObjects engine comparing to other engines.

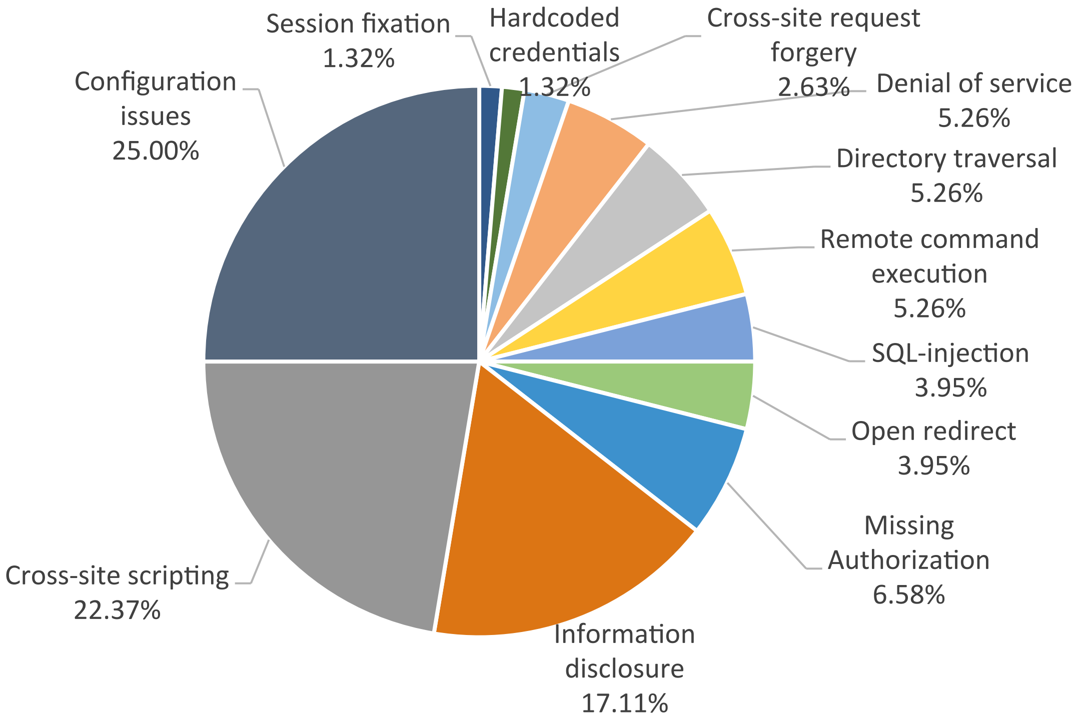

Figure 5.4-1 SAP Security Notes sorted by types in SAP BusinessObjects

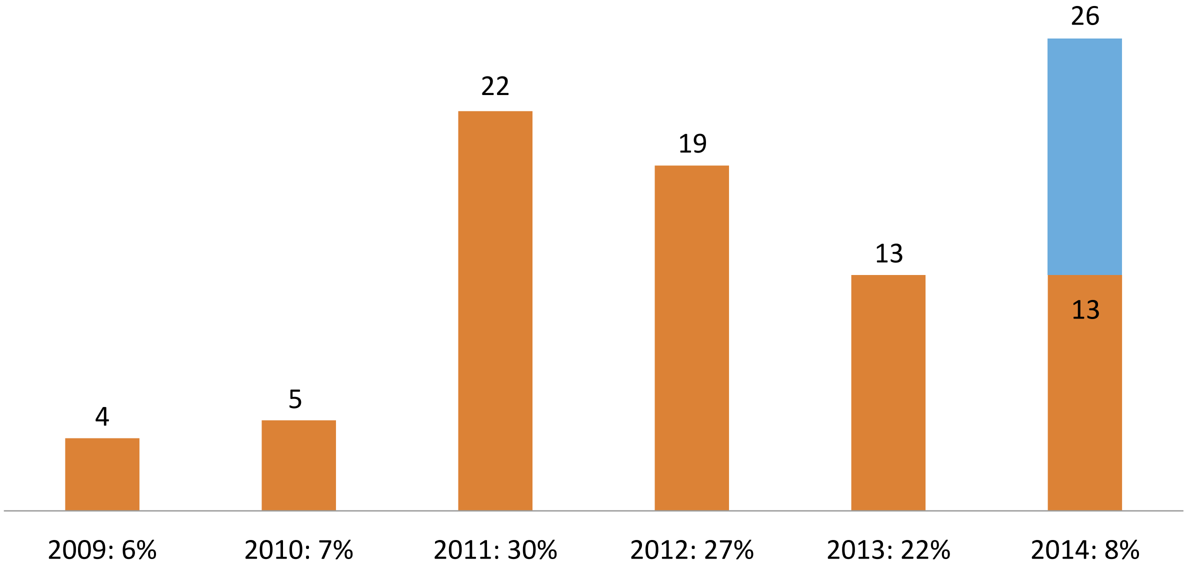

Figure 5.4-2 SAP Security Notes sorted by years in SAP BusinessObjects

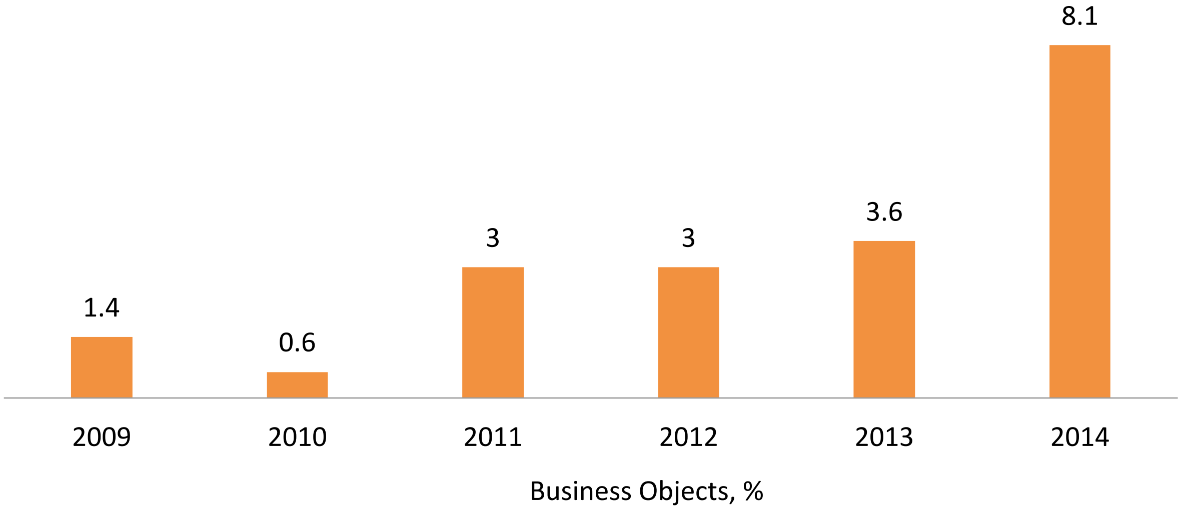

Figure 5.4-3 SAP Security Notes in SAP BusinessObjects compared to all security notes by year

5.5. SAP Frontend platform (SAPGui)

All client-side products, which include SAP Frontend (SAPGUI) JAVA Gui, SAP NetWeaver Business Client (NWBC). Here we clearly see that frontend applications very different to server-side in terms of vulnerabilities. More than ¼ of vulnerabilities – are memory corruption and buffer overflow issues.

However if we look at trend we will see that the number of vulnerabilities is decreasing dramatically down to 0 in 2014 comparing to their peak in 2009-2010 when we started deep research in SAP GUI security in early 208'th and uncover most of the dangerous vulnerabilities. Details of that research can be found here [6].

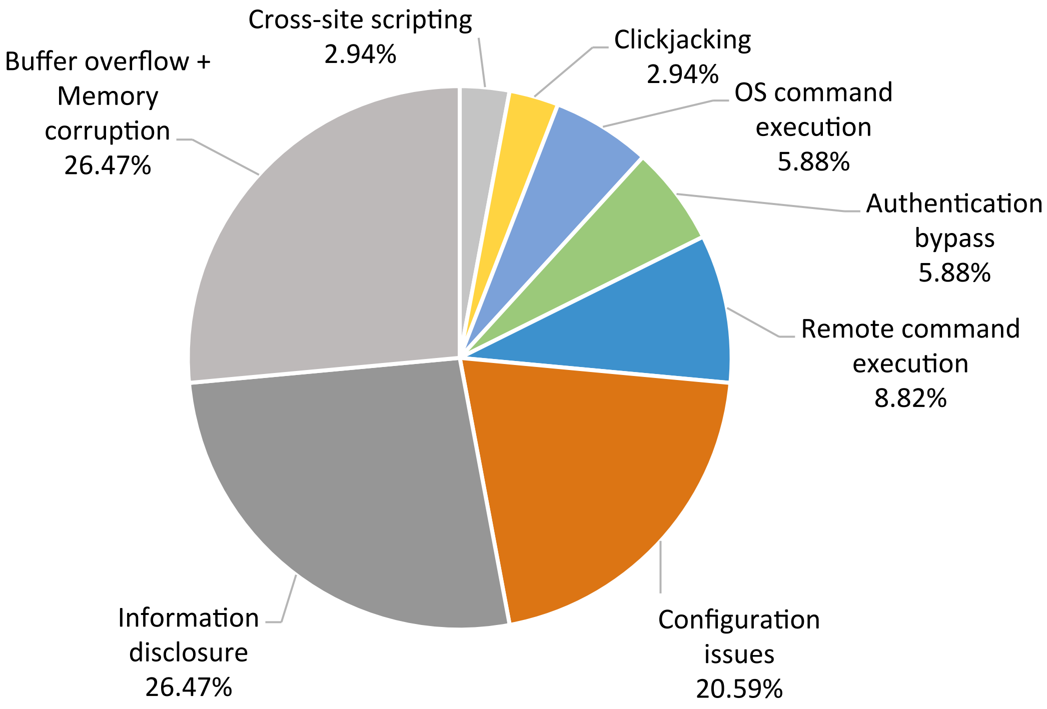

Figure 5.5-1 SAP Security Notes sorted by types in SAP Frontend

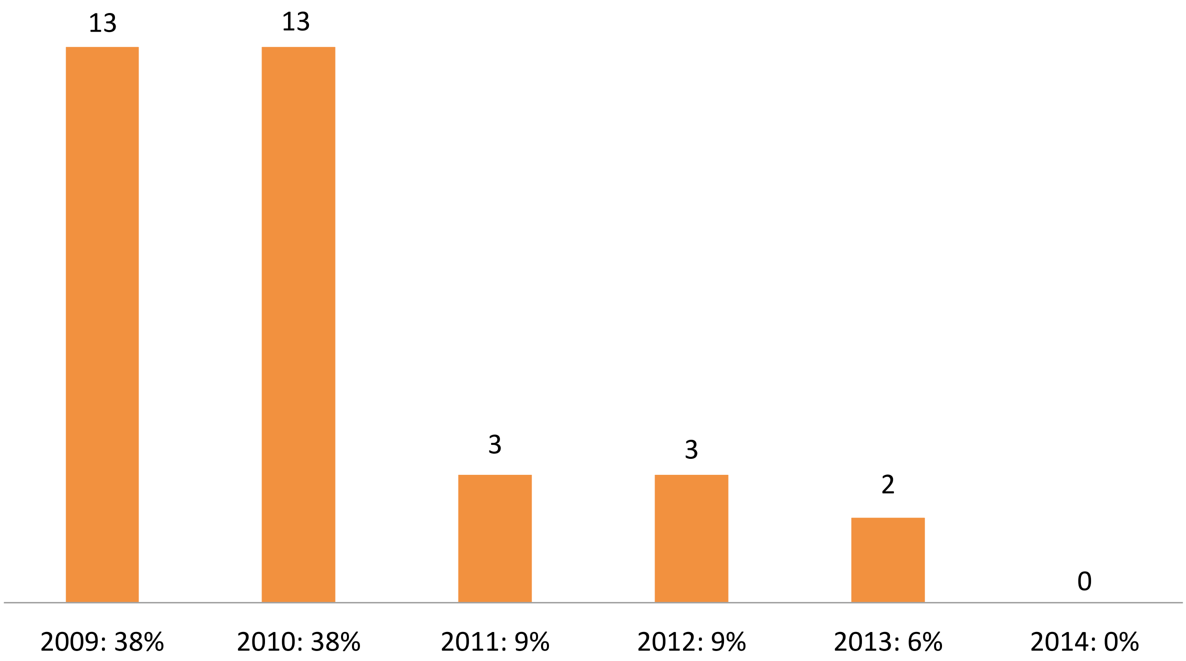

Figure 5.5-2 SAP Security Notes sorted by years in SAP Frontend

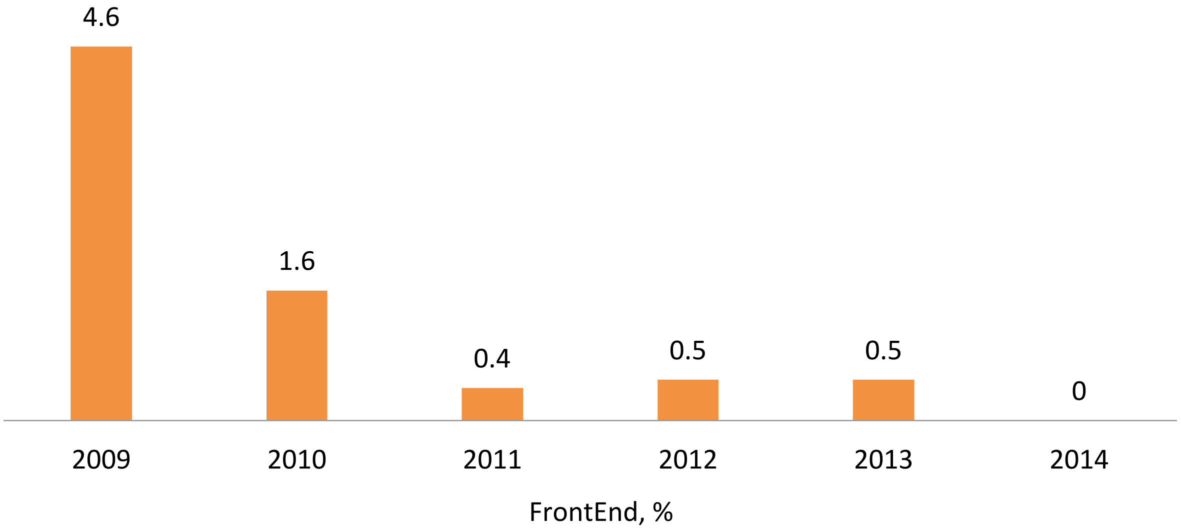

Figure 5.5-3 SAP Security Notes in SAP Frontend compared to all security notes by year

Analysis of 3000 vulnerabilities in SAP

Thus, having collected information on all of these engines we can see the following table*:

*Results presented on this table may slightly vary due to fact that for some of vulnerabilities description is not clear.

Vulnerability type	SAP NW ABAP	SAP NW J2EE	SAP HANA	SAP Business Objects	SAP Frontend	SUM
Cross-site scripting	481	148	**1**	17	1	648
Missing authorization	522	49	**1**	5	0	577
Directory traversal	367	28	0	4	0	399
Configuration issues	215	69	**5**	19	7	315
SQL-injection	220	13	1	3	0	237
Cross-site request forgery	176	40	0	2	0	218
Information disclosure	84	83	0	13	9	189
Code injection	105	5	1	0	0	111
Hardcoded credentials	94	5	0	1	0	100
Denial of service	28	14	0	4	0	46
Buffer overflow	22	5	0	0	9	36
Verb tampering	2	21	0	0	0	23
Remote command execution	10	5	0	4	3	22
Authentication bypass	10	7	**1**	0	2	20
XML external entity	7	8	0	0	0	15
SMB relay	5	3	0	0	0	8
Open redirect	3	2	0	3	0	8
Session fixation	2	5	0	1	0	8
OS command execution	4	1	0	0	2	7
HTTP response splitting	3	1	0	0	0	4
Local command execution	3	0	0	0	0	3
Clickjacking	0	1	0	0	1	2
TOTAL	**2363**	**513**	**10**	**76**	**34**	**2996**
ABSOLUTE TOLAL	**TOTAL (2996)+UNKNOWN(17)**					**3013**

Table 4.1. SAP Security Notes sorted by types in engines

6. Conclusion

Old issues are being patched but many new systems have vulnerabilities. Number of vulnerabilities per year going down compared to 2010, but they are more critical. Number of companies who search for issues in SAP is growing so we can conclude that interest to SAP platform security has been growing exponentially and there are positive points of that, for example – latest SAP products are more secure by default. 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. And while so many issues have already been closed there are much more areas which are still not covered by researchers and where can be lots of 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. This area has been changed a lot during last year and SAP now investing much more resources and money for internal SDLC processes and internal Security conferences.

Unfortunately, as a year ago, the main mission still lies on administrators who should enforce security of their SAP systems by using guidelines, secure configuration, patch management, code review and continuous monitoring.

About ERPScan

ERPScan is a most honored ERP security provider founded in 2010 and engaged in the research of ERP security, particularly in SAP. The company develops products for SAP system security. ERPScan is the leading SAP AG partner in discovering and solving security vulnerabilities. Apart from this, the company renders consulting services for secure configuration, development and implementation of SAP systems which are used by SAP AG and Fortune 2000 companies, and also conducts comprehensive assessments and penetration testing of custom solutions.

Our flagship product "ERPScan Security Monitoring Suite for SAP" is an award-winning product for automatic assessment of SAP platform security, ABAP code review and standard compliance. This software is the only solution on the market to assess and monitor four tiers of SAP security: vulnerability assessment, source code review, SoD conflicts. It is successfully used by the largest companies from industries like oil and gas, nuclear, banking, logistics, and avionics as well as by consulting companies. ERPScan Security Monitoring Suite is a unique product which enables conducting a complex security assessment and monitoring SAP security afterwards.

The company’s expertise is based on research conducted by the ERPScan research center – a subdivision of ERPScan. It is engaged in vulnerability research and analysis of business-critical applications, particularly SAP. SAP AG gives acknowledgements to security researchers from ERPScan almost every month on their website.

ERPScan experts are frequent speakers in prime International conferences held in the USA, EUROPE, CEMEA and ASIA such as BlackHat, HITB, HackerHalted, SourceBarcelona, DeepSEC, CONFidence, Troopers, T2, InfoSecurity and many more. ERPScan researchers have gained multiple acknowledgements from key software vendors such as SAP, Oracle, IBM, VMware, Adobe, HP, Kaspersky, Apache, Alcatel and others for finding vulnerabilities in their solutions.

ERPScan has highly qualified experts in staff, who have experience in numerous different fields of security, from web applications and reverse engineering to industrial systems and embedded/mobile solutions, accumulating their experience to expand the research of SAP security.

About EAS-SEC

Project

EAS-SEC (formerly part of the global strategy group OWASP Projects) [47], a non-profit worldwide organization focused on improving business application software security.

EAS-SEC is a guide for people involved in the acquisition, design and implementation of large-scale applications, the so-called Enterprise Applications. Security of Enterprise Applications is one of the most discussed topics in the general area of Applications security. This is due to the fact that such applications control the organization resources including funds which may be lost as a result of any breach of security.

Project mission

The purpose of the EAS-SEC project launched in 2010 is increase of awareness of business application and enterprise applications security problems for users, administrators and developers and also the creation of guidelines and tools to assess the safety, security, safe set-up and development of enterprise applications. The general analysis of the main business applications was carried out and key areas of safety to which it is necessary to pay attention both when developing and at introduction are collected. In addition, there were two researches–«SAP Security in figures for 2011» [48] and «The state of SAP security 2013: Vulnerabilities, threats and trends» [49]. The results of these reports have been presented at key conferences such as RSA and have been highlighted in the press [50].

The EAS-SEC has a number of the main objectives on the basis of which subprojects are created:

1. Notification of broad masses about vulnerabilities of safety of corporate appendices, on means of release of annual statistics of vulnerabilities of safety of corporate appendices. Subproject: Enterprise Business Application Vulnerability Statistics [51];

2. Help to the companies, engaged in release of the software, increase of safety of their solutions, providing tools for the Enterprise Business Application Vulnerability Assessment Guide [52] subproject;

3. Development of free extended tools for an assessment of safety of corporate appendices, and for the Enterprise Business Application Development Issues [53] subproject;

Links and future reading

[1] «ERPScan – strategic SAP AG partner in security» [Internet]. Available: http://erpscan.com/.

[2] «OWASP-EAS» [Internet]. Available: http://eas-sec.org/.

[3] «Worldwide Public statistics of SAP systems» [Internet]. Available: http://sapscan.com/.

[4] «As economy falters, employee theft on the rise» [Internet]. Available: http://www.lasvegassun.com/news/2009/nov/06/managing-fraud-lesson-recession/.

[5] «ACFE Report to the Nations» [Internet]. Available: https://chapters.theiia.org/birmingham/Documents/Fraud___Internal_Audit_IIA_6Sep2012.pdf.

[6] «ERPScan publications: "SAP Security: attacking SAP clients"» [Internet]. Available: http://erpscan.com/publications/sap-security-attacking-sap-clients/.

[7] «CanSecWest conference report by Steve Lord, Mandalorian» [Internet]. Available: cansecwest.com/slides06/csw06-lord.ppt.

[8] «ERPScan's SAP Pentesting Tool» [Internet]. Available: http://erpscan.com/products/erpscan-pentesting-tool/.

[9] «ERPScan WEBXML Checker» [Internet]. Available: http://erpscan.com/products/erpscan-webxml-checker/.

[10] «Sapyto – SAP Penetration Testing Framework» [Internet]. Available: cybsec.com/EN/research/sapyto.php.

[11] «Top 10 most interesting SAP vulnerabilities and attacks» [Internet]. Available: http://erpscan.com/wp-content/uploads/2012/06/Top-10-most-interesting-vulnerabilities-and-attacks-in-SAP-2012-InfoSecurity-Kuwait.pdf.

[12] «Acknowledgments to Security Researchers» [Internet]. Available: http://scn.sap.com/docs/DOC-8218.

[13] «Vulnerability Database Security Focus» [Internet]. Available: securityfocus.com.

[14] «Common Vulnerabilities and Exposures» [Internet]. Available: http://cve.mitre.org.

[15] «US National Vulnerability Database» [Internet]. Available: http://web.nvd.nist.gov/.

[16] «Exploit Database by Offensive Security» [Internet]. Available: http://exploit-db.com.

[17] «SAP NetWeaver J2EE – DilbertMSG SSRF» [Internet]. Available: http://erpscan.com/advisories/dsecrg-12-036-sap-xi-authentication-bypass/.

[18] «SAP Host Control – Command injection» [Internet]. Available: http://contextis.com/research/blog/sap-parameter-injection-no-space-arguments/.

[19] «SAP NetWeaver J2EE – File Read/Write» [Internet]. Available:

https://service.sap.com/sap/support/notes/1682613.

[20] «SAP Message Server – Buffer Overflow» [Internet]. Available: http://www.zerodayinitiative.com/advisories/ZDI-12-112/ .

[21] «SAP Dispatcher – Diag protocol Buffer Overflow» [Internet]. Available: http://www.coresecurity.com/content/sap-netweaver-dispatcher-multiple-vulnerabilities.

[22] «Uncovering SAP vulnerabilities: Reversing and breaking the Diag protocol» [Internet]. Available: corelabs.coresecurity.com/index.php?module=Wiki&action=attachment&type=publication&page=Uncovering_SAP_vulnerabilities_reversing_and_breaking_the_Diag_protocol&file=Slides.pdf.

[23] «SAP Management Console Information Disclosure» [Internet]. Available: http://www.onapsis.com/get.php?resid=adv_onapsis-2011-002.

[24] «Systems Applications Proxy Pwnage» [Internet]. Available: http://www.sensepost.com/cms/resources/labs/tools/poc/sapcap/44con_2011_release.pdf.

[25] «Architecture and program vulnerabilities in SAP's J2EE engine» [Internet]. Available: http://erpscan.com/wp-content/uploads/2011/08/A-crushing-blow-at-the-heart-SAP-J2EE-engine_whitepaper.pdf.

[26] «The ABAP Underverse» [Internet]. Available: http://virtualforge.com/tl_files/Theme/whitepapers/BlackHat_EU_2011_Wiegenstein_The_ABAP_Underverse-WP.pdf.

[27] «SQL Injection with ABAP» [Internet]. Available: http://virtualforge.com/tl_files/Theme/Presentations/HITB2011.pdf.

[28] «SAP NetWeaver – Authentication bypass (Verb Tampering)» [Internet]. Available: http://erpscan.com/advisories/dsecrg-11-041-sap-netweaver-authentication-bypass-verb-tampering/.

[29] «Invoker Servlet» [Internet]. Available: http://help.sap.com/saphelp_nw70ehp2/helpdata/en/bb/f2b9d88ba4e8459e5a69cb513597ec/frameset.htm.

[30] «PROTECTING JAVA AND ABAP BASED SAP APPLICATIONS AGAINST COMMON ATTACKS» [Internet]. Available: http://virtualforge.com/tl_files/Theme/whitepapers/201106_SAP_Security_Recommendations_Protecting_JAVA_ABAP.pdf.

[31] «SAP Infrastructure security internals: Google and Shodan hacking for SAP» [Internet]. Available: http://erpscan.com/press-center/blog/sap-infrastructure-security-internals-google-and-shodan-hacking-for-sap/.

[32] «SAP Application Server Security essentials: default passwords» [Internet]. Available: http://erpscan.com/press-center/blog/sap-application-server-security-essentials-default-passwords/.

[33] «SAP NetWeaver SLD – Information Disclosure» [Internet]. Available:

http://erpscan.com/advisories/dsecrg-11-023-sap-netweaver-sld-information-disclosure/.

[34] «NetWeaver BCB – Missing Authorization / Information disclosure» [Internet]. Available: http://erpscan.com/advisories/dsecrg-11-027-netweaver-bcb-%E2%80%93-missing-authorization-information-disclosure/.

[35] «SAP NetWeaver AdapterFramework – information disclosure» [Internet]. Available: http://erpscan.com/advisories/dsecrg-12-050-sap-netweaver-adapterframework-information-disclosure/.

[36] «ops$ mechanism» [Internet]. Available: http://scn.sap.com/community/oracle/blog/2012/10/15/sunset-for-ops-mechanism-no-more-supported-by-oracle-not-used-by-sap.

[37] «Easy Service Marketplace» [Internet]. Available: http://www.easymarketplace.de/saprouter.php.

[38] «SAP NetWeaver SOAP RFC – Denial of Service / Integer overflow» [Internet]. Available: http://erpscan.com/advisories/dsecrg-11-029-sap-netweaver-soap-rfc-%E2%80%93-denial-of-service-integer-overflow/.

[39] «SAP Netweaver XRFC — Stack Overflow» [Internet]. Available: http://erpscan.com/advisories/dsecrg-10-005-sap-netweaver-xrfc-%E2%80%94-stack-overflow/.

[40] «TCP/IP Ports Used by SAP Applications» [Internet]. Available: http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/4e515a43-0e01-0010-2da1-9bcc452c280b?QuickLink=index&overridelayout=true&42472931642836.

[41] «Scrubbing SAP clean with SOAP» [Internet]. Available: http://www.slideshare.net/ChrisJohnRiley/sap-insecurity-scrubbing-sap-clean-with-soap.

[42] «CORE Labs Discovery of Six Vulnerabilities within SAP Netweaver» [Internet]. Available: http://blog.coresecurity.com/2012/05/09/core-labs-discovery-of-six-vulnerabilities-within-sap-netweaver/.

[43] «Fighting Economic Crime in the Financial Services sector» [Internet]. Available: http://docs.media.bitpipe.com/io_10x/io_102267/item_485936/Economic%20crime%20in%20FS%20sector.pdf.

[44] «Espionage virus sent blueprints to China» [Internet]. Available: http://www.telegraph.co.uk/technology/news/9346734/Espionage-virus-sent-blueprints-to-China.html.

[45] «Win32/Spy.Ranbyus modifying Java code in RBS Ukraine systems» [Internet]. Available: http://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/.

[46] «Associated Press Twitter Account Hacked in Market-Moving Attack» [Internet]. Available: http://www.bloomberg.com/news/2013-04-23/dow-jones-drops-recovers-after-false-report-on-ap-twitter-page.html.

[47] «The Open Web Application Security Project (OWASP)» [Internet]. Available: https://www.owasp.org/index.php/Main_Page.

[48] «SAP Security In Figures – A Global Survey 2007-2011» [Internet]. Available: http://erpscan.com/publications/sap-security-in-figures-a-global-survey-2007-2011/

[49] «The state of SAP security 2013: Vulnerabilities, threats and trends» [Internet]. Available: http://www.rsaconference.com/writable/presentations/file_upload/das-t03_final.pdf.

[50] G. Burton, «Companies exposed to attack by out-of-date SAP applications» [Internet]. Available: http://www.computing.co.uk/ctg/news/2275640/companies-exposed-to-attack-by-outofdate-sap-applications.

[51] «Enterprise Business Application Vulnerability Statistics» [Internet]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Vulnerability_Statistics.

[52] «Enterprise Business Application Security Vulnerability Testing Guide» [Internet]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Security_Vulnerability_Testing_Guide_v1.

[53] «Enterprise Business Application Security Software» [Internet]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Security_Software.

[54] «Enterprise Business Application Security Implementation Assessment Guide» [Internet]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Security_Implementation_Assessment_Guide.

[55] «The ERP Security Challenge» [Internet]. Available: http://www.cio.com/article/216940/The_ERP_Security_Challenge.

Our contacts

E-mail: info@erpscan.com

PR: press@erpscan.com

Web: www.erpscan.com