onapsis
Securing Business Essentials

Cyber-Attacks & SAP® Systems

Is our business-critical infrastructure exposed?

Mariano Nunez

mnunez@onapsis.com

March 15th, 2012

BlackHat Europe 2012

Disclaimer

This publication is copyright 2012 Onapsis, Inc. – All rights reserved.

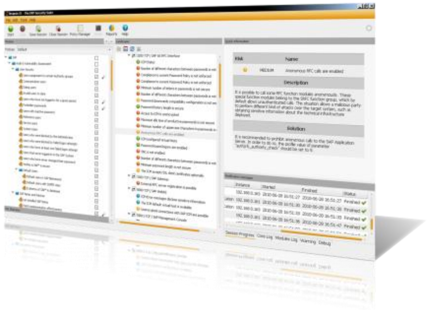
This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Who is Onapsis, Inc.?

- Company focused in the **security of ERP systems and business-critical infrastructure** (**SAP®,** Siebel®, Oracle® E-Business SuiteTM, PeopleSoft®, JD Edwards® …).
- Working with Global Fortune-100 and large governmental organizations.
- What does Onapsis do?
  - Innovative ERP security software (Onapsis X1, Onapsis Bizploit, Onapsis IA).
  - ERP security consulting services.
  - Trainings on business-critical infrastructure security.



Who am I?

- **Co-founder & CEO** at **Onapsis.**
- Discovered 50+ **vulnerabilities** in SAP, Microsoft, IBM, ...
- **Speaker/Trainer** at BlackHat, RSA, HackerHalted, HITB, Ekoparty, DeepSec, ...
- Developer of the first **opensource SAP/ERP PenTesting frameworks**.
- Lead author of the “SAP Security In-Depth” publication.

Agenda

- Introduction
- A dangerous status-quo
- External and internal threats
- The current security level of SAP implementations
- The TOP-11 vulnerabilities affecting the SAP infrastructure
- Defending the SAP platform
- Conclusions

Introduction

What is SAP?

- **Largest** provider of **business management solutions** in the world.
  - More than 140.000 implementations around the globe.
  - More than 90.000 customers in 120 countries.

- Used by **Global Fortune-1000 companies**, **governmental organizations** and **defense agencies** to **run their every-day business processes.**
  - Such as Revenue / Production / Expenditure business cycles.

FINANCIAL PLANNING TREASURY PAYROLL

INVOICING LOGISTICS

SALES BILLING

PRODUCTION PROCUREMENT

A Dangerous Status-quo

What “SAP Security” used to be 5 years ago

- **“SAP security” was regarded as a synonym of “Segregation of Duties controls”.**
    - **Sample goal:** “Make sure that if Tim can create a new vendor, he can not create purchase orders”.
    - This was mapped to a SoD matrix with SAP transactions / authorization objects.

- Most large organizations had “SAP Security” in place: they were **spending hundreds of thousands/millions of dollars in SAP security yearly** by having:
    - A dedicated Team of SAP security professionals.
    - SoD & GRC software (usually costing **$500K-$2M or more**).

Breaking the status-quo / BlackHat 2007

- The Information Security and Audit communities were doing fine with that status quo. Most SAP-related security documents and guidelines only dealt with SoD issues.

- One day, back in 2005, we were hired to do a Webapp pentest.
- The only difference was that the Web Server was an SAP Web Application Server.
- Suddenly, we started discovering vulnerabilities that were not in the apps, but in the framework itself!
- We checked online… they were not reported.
- Back then, the total number of reported SAP vulnerabilities was: 90

What “SAP Security” really is

- SAP security is a complex discipline, that must be addressed holistically!
- SoD controls are necessary, but **they are not enough**.
- They only address one of the layers where security must be enforced.

- **The forgotten layer: The Business Infrastructure (NetWeaver/Basis).**
  - Base framework in charge of **critical tasks** such as authentication, authorization, encryption, interfaces, audit, logging, etc.
  - Can be susceptible of security vulnerabilities that, if exploited, can lead to **espionage, sabotage and fraud attacks** to the business information.

A different (higher) risk profile

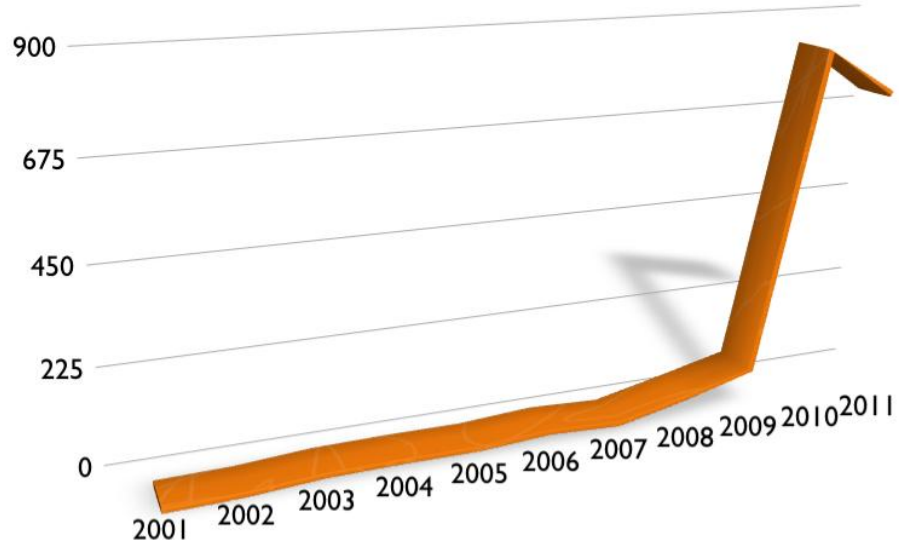
- **Exploitation of a SoD weakness:**
  1. The attacker needs a *valid user account* in the target SAP system.
  2. He needs to find out that he has more access than he should have.
  3. Common auditing features may detect his activities.

- **Exploitation of a technical/infrastructure weakness:**
  1. The attacker **does not need** a *valid user account* in the target SAP system.
  2. **A successful attack will allow him to achieve SAP_ALL privileges** (even without having a real user!).
  3. Common auditing features **would not** detect his activities.

A Rising Threat

- **The number of SAP Security Notes** has increased dramatically over the last years.
- Security Notes usually address one or more vulnerabilities.
- Most of these issues affect the *Business Runtime.*

Number of SAP Security Notes per Year

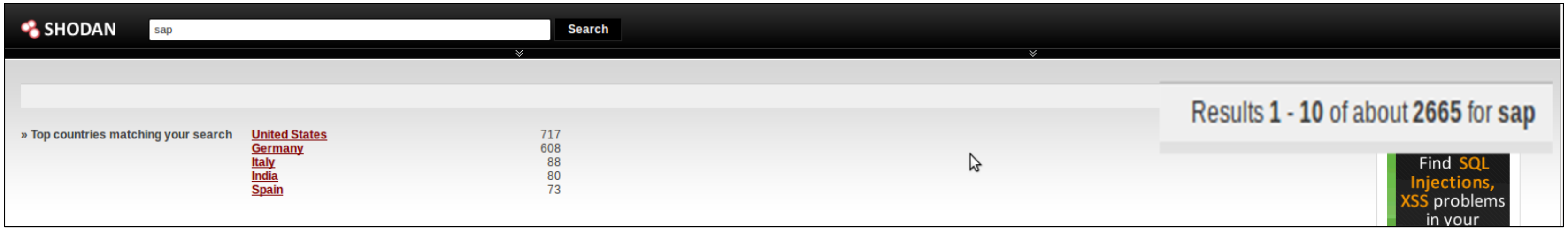


External and Internal Threats

Querying search engines

- While most SAP systems were only reachable internally a decade ago, now it's common for **SAP systems to be connected to the Internet.**

- **Attackers know how to find them** using regular search engines.

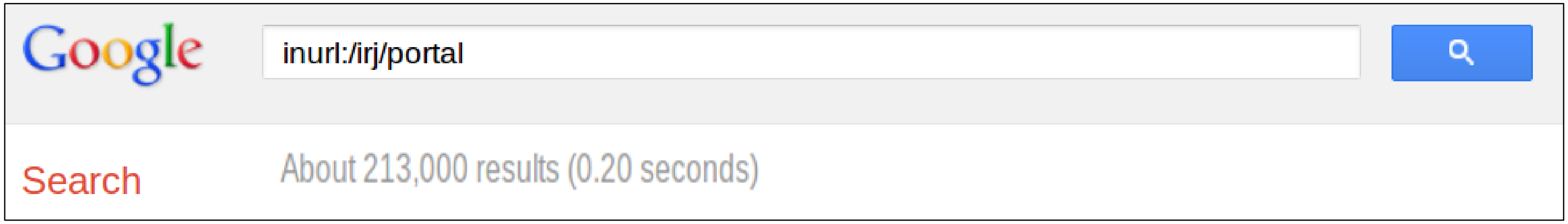


Results 1 - 10 of about 2665 for sap

» Top countries matching your search

United States	717
Germany	608
Italy	88
India	80
Spain	73

Find SQL Injections, XSS problems in your



About 213,000 results (0.20 seconds)

But… is it more than just Web apps?

- Even if companies believe they are not online, many of them are!
- When you acquire SAP, the agreement specifies that you have to allow remote access through a special component called **SAProuter.**

- Network services such as the Dispatcher, Gateway, Management Console, Message Server, P4 interface, etc. should never touch the Internet…

- **What's the reality?**

- From the Trenches - The Current Security Level of SAP Implementations

From the trenches

- Since 2005, our experts were engaged to perform numerous SAP Penetration Tests, including some of the largest organizations of the world.
- We have evaluated 550+ SAP Application Servers in total.

- A typical project:
  - Network access to the end-user network.
  - List of IP addresses of SAP servers.
  - NO user/password credentials.

From the trenches

- Our findings:
  - Over 95% of the systems were exposed to espionage, sabotage and fraud attacks. A malicious party would have been able to achieve SAP_ALL or equivalent privileges without having access credentials.
  - Only 5% of the evaluated SAP systems had the proper security audit logging features enabled.
  - None of the evaluated SAP systems were fully updated with the latest SAP security patches.
  - In most cases, the attack vectors that leaded to the initial compromise comprised the exploitation of vulnerabilities that have been in the public domain for more than 5 years.

The TOP-11 vulnerabilities affecting the SAP infrastructure

BIZEC.org, the business application security initiative

- **BIZEC.org** is a **non-profit organization** focused on security threats affecting ERP systems and business-critical infrastructure.

- The **BIZEC TEC/11** project lists the most common and most critical security defects and threats affecting the Business Runtime layer/infrastructure of SAP platforms.

BIZEC TEC-01: Vulnerable Software in Use

Risk

The SAP platform is running based on technological frameworks whose versions are affected by reported security vulnerabilities and the respective fixes have not been applied.

Business Impact

Attackers would be able to exploit reported security vulnerabilities and perform unauthorized activities over the business information processed by the affected SAP system.

BIZEC TEC-02: Standard Users with Default Passwords

Risk

Users created automatically during the SAP system installation, or other standard procedures, are configured with default, publicly known passwords.

Business Impact

Attackers would be able to login to the affected SAP system using a standard SAP user account. As these accounts are usually highly privileged, the business information would be exposed espionage, sabotage and fraud attacks.

BIZEC TEC-03: Unsecured SAP Gateway

Risk

The SAP Application Server's Gateway is not restricting the starting, registration or cancellation of external RFC servers.

Business Impact

Attackers would be able to obtain full control of the SAP system. Furthermore, they would be able to intercept and manipulate interfaces used for transmitting sensitive business information.

BIZEC TEC-04: Unsecured SAP/Oracle authentication

Risk

The SAP ABAP Application Server authenticates to the Oracle database through the OPS$ mechanism, and the Oracle's listener has not been secured.

Business Impact

Attackers would be able to obtain full control of the affected SAP system's database, enabling them to create, visualize, modify and/or delete any business information processed by the system.

BIZEC TEC-05: Insecure RFC interfaces

Risk

The SAP environment is using insecure RFC connections from systems of lower security-classification level to systems with higher security-classification levels.

Business Impact

Attackers would be able to perform RFC pivoting attacks, by first compromising an SAP system with low security-classification and, subsequently, abusing insecure interfaces to compromise SAP systems with higher security-classification levels.

BIZEC TEC-06: Insufficient Security Audit Logging

Risk

The SAP System's auditing features are disabled or not properly configured.

Business Impact

It would not be possible to detect suspicious activities or attacks against the SAP system. Furthermore, valuable information for forensic investigations would not be available.

BIZEC TEC-07: Unsecured SAP Message Server

Risk

The SAP System's Message Server is not restricting the registration of SAP Application Servers.

Business Impact

Attackers would be able to register malicious SAP Application Servers and perform man-in-the-middle attacks, being able to obtain valid user access credentials and sensitive business information. Attacks against user workstations would also be possible.

BIZEC TEC-08: Dangerous SAP Web Applications

Risk

The SAP Application Server is allowing access to Web applications with reported security vulnerabilities or sensitive functionality.

Business Impact

Attackers would be able to exploit vulnerabilities in such Web applications, enabling them to perform unauthorized activities over the business information processed by the affected SAP system.

BIZEC TEC-09: Unprotected Access to Administration Services

Risk

The SAP Application Server is not restricting access to sensitive administration or monitoring services.

Business Impact

Attackers would be able to access administration or monitoring services and perform unauthorized activities over the affected SAP systems, possibly leading to espionage and/or sabotage attacks.

BIZEC TEC-10: Insecure Network Environment

Risk

The network environment of the SAP platform is not properly secured through the deployment and configuration of network firewalls, specialized Intrusion Prevention and Detection systems and application-layer gateways.

Business Impact

Attackers would be able to access sensitive SAP network services and possibly exploit vulnerabilities and unsafe configurations in them, leading to the execution of unauthorized activities over the affected SAP platform.

BIZEC TEC-11: Unencrypted Communications

Risk

The confidentiality and integrity of communications in the SAP landscape is not enforced. These communications comprise SAP-to-SAP connections as well as interactions between SAP servers and external systems, such as user workstations and third-party systems.

Business Impact

Attackers would be able to access sensitive technical and business information being transferred to/from the SAP environment.

Defending the SAP Platform

The Challenges

- **Knowledge.** Understanding how to assess and secure an SAP system requires specialized knowledge.

- **Scope.** The *entire* platform must be secured. This comprises:
  - Every Landscape (ERP, CRM, SCM, …) in the organization
    - Every SAP system in each landscape
      - Every Client (mandant) and AS in each system
        - Every of the 1500+ configuration parameters of each AS

- **Periodicity.** The security of the SAP infrastructure must be evaluated periodically, at least after each SAP Security Patch Day, to verify whether new risks have been raised and evaluate mitigation actions.

SAP Security - Who is responsible?

- Unlike other systems (such as Web servers, domain controllers, etc.), the security of SAP systems usually falls under the domain of “The Business”.

- This means that the officers in charge of securing the systems are the same ones who are responsible for verifying whether they are secure or not. → **FAIL.**

- **If the organization's SAP teams are responsible for protecting the SAP platform, the Information Security Manager / CISO department must verify whether the current security level matches the organization's defined risk appetite.**

SAP Security - Who is responsible?

Let’s think about it:

- Is the SAP platform a “blackbox” for the Information Security team?
- Does the Information Security team “trust but verify”?
- Who will be ultimately responsible if there is a security breach in the SAP platform?
- What if the SAP platform is compromised, not by a high-profile and complex attack, but rather as the result of the exploitation of a vulnerability that has been publicly known for several years?

Conclusions

Conclusions

- **Segregation of Duties controls** are necessary, **but not enough!**
- The SAP infrastructure can be exposed to **technical security vulnerabilities** that, if exploited, would enable **espionage, sabotage** and **financial fraud** attacks.
- The risk level in this matter is higher, **as attackers do not even need a user account in the system!**
- The number of SAP security notes have dramatically increased over the last years. Customers are not catching-up.
- Many companies state that “our SAP system has not been hacked”, but they do not even have the basic auditing features enabled!

Conclusions

- **Many SAP systems are connected to the Internet, and exposing sensitive services beyond Web applications.** Furthermore, the internal network is usually not properly segmented.

- **SAP is taking important steps into increasing the security of its customers' systems** (security guides, regular patches, new standards).

- While "The Business" may work on the security of the platform, it's the responsibility of Information Security to verify that they are doing their job.

- If our business-critical infrastructure is hacked by a 5-year-old vulnerability, we are clearly doing something wrong.

Questions?

mnunez@onapsis.com

@marianonunezdc

Thank you!

www.onapsis.com

Follow us! @onapsis