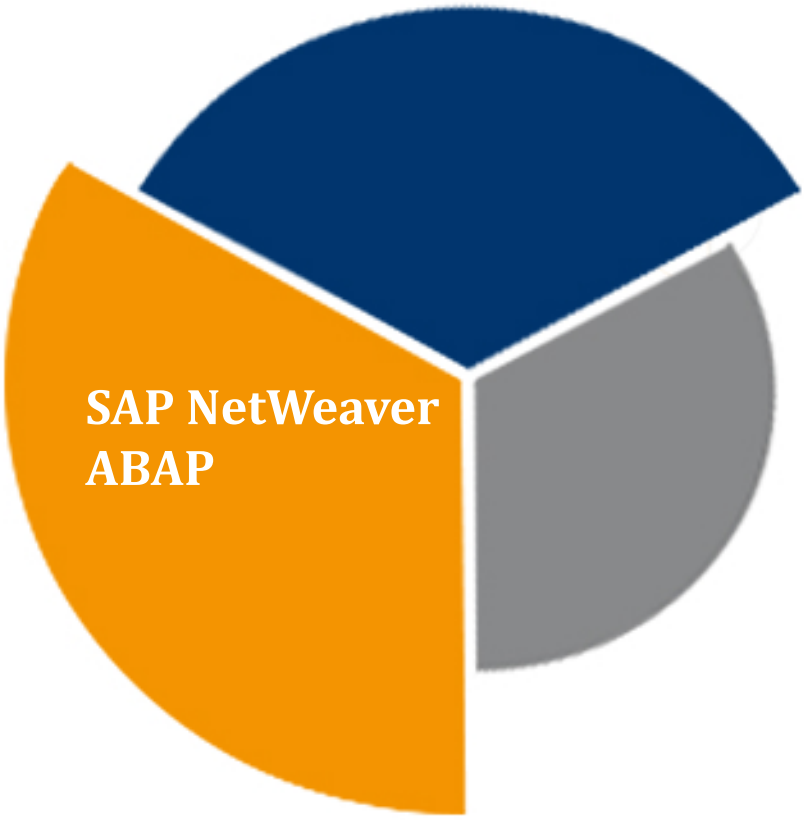
ERPScan

[EASSEC-PVAG-ABAP] THE SAP NETWEAVER ABAP PLATFORM VULNERABILITY ASSESSMENT GUIDE



Authors:
Alexander Polyakov
Kirill Nikitenkov
Contributed by:
Nikolai Mescherin
Eugene Neyelov
Dmitry Chastukhin

ENTERPRISE APPLICATION SOFTWARE SECURITY PROJECT
APPLICATION IMPLEMENTATION ASSESSMENT GUIDE FOR ABAP

version 2014

Contents

Disclaimer

According to partnership agreement with the SAP, we do not have the right to publish any detailed information about the found vulnerabilities before an official support package or a SAP Note is issued. That is why this document includes a detailed description of those vulnerabilities only that we currently have the right to disclose. However, the exploitation examples of all mentioned vulnerabilities are available in the conference videos and at erpscan.com [1].

Introduction

The ERP system is in the core of any large company: it deals with all processes critical for business – purchases, payments, logistics, HR, product management, financial planning etc. All information stored in the ERP systems is sensitive, and any unauthorized access to this information can cause huge damages up to a business interruption.

According to the report by the Association of Certified Fraud Examiners (ACFE [2]), in 2006 - 2010, the organizations losses caused by the internal fraud (the IT-frauds) amounted to app. 7% of annual revenue [3].

For the last five years, a widespread myth that the ERP security is only a SOD matrix was over, and today this belief seems to become a history for many people. For that time, the SAP security experts have presented lots of detailed reports on various attacks on the internal SAP subsystems:
— the RFC protocol,
— the SAP ROUTER access control system,
— the SAP web-applications,
— the SAP GUI client workstations, and many others.

The interest for this area grows exponentially every year: compared to only 1 report on SAP Security [5] in 2006, more than 30 of such reports were presented in 2013 at specialized hacking and security technical conferences. Lately, a number of hacking utilities were released, and thus confirmed the possibility of attacks on the SAP solutions [6] [7] [8].

According to the business application vulnerability statistics [11] [12], more than one hundred vulnerabilities in the SAP products were fixed in 2009, while this figure was more than 500 in 2010. In August 2013, there were more than 2700 SAP Security Notes, i.e. notifications on various SAP components vulnerabilities.

The EAS-SEC Project

The open security project

The **EAS-SEC** Project *(Enterprise Application Systems Security Project)* is a non-profit project devoted to the Enterprise Application System Security. [9] Named as OWASP-EAS, it also became a part of the global group **OWASP** *(The Open Web Application Security Project)*[10], which is a worldwide non-profit organization looking forward to increasing the software security level.

The EAS-SEC is a guide for people participating in design, implementation or development of the large-scale applications, the so-called enterprise applications systems. The enterprise application system security is one of the most discussed subjects in the entire security field, since such application systems, while performing their major functions, control the organization resources, including funds, where a material loss can be a result of any security breach.

The project objectives

The objectives of the EAS-SEC project launched in 2010 are:
— raising user, administrator and business application developer awareness of the enterprise application system security problems,
— development of guidance and secure configuration tools , and
— development of enterprise application systems .

Currently, major business applications were analyzed in general and the key security areas were compiled to consider upon the development and implementation processes. Besides, two studies were carried out:
— *SAP Security in Figures 2011* [11]

— *SAP Security in Figures 2013* [12]

These reports were presented at key conferences such as RSA APAC and were published in the mass media [13].

This document is aimed to raise administrator, security and implementation experts awareness of how to configure the SAP NetWeaver ABAP securely, and to assist them in basic vulnerability assessment of the SAP solution to protect against major threats.

Business applications are very complex and huge systems with a number of components such as DBMS, application and web-servers, client software and so on. Any of these levels may contain vulnerabilities and configuration errors that enable an adversary to get an unauthorized access to a system.

The data of the most widespread and critical vulnerabilities were collected and rated on our vulnerability studies of the most popular business applications, such as SAP NetWeaver ABAP, SAP NetWeaver J2EE, Oracle E-Business Suite, Oracle PeopleSoft, JD Edwards, Microsoft Dynamix and others less known.

The Assessment Guide

The EAS-SEC project has a range of major goals, on which the following subprojects are based:

1. To raise public awareness of the enterprise application system security vulnerabilities by publication of the relevant annual statistics . The subproject: *Enterprise Business Application Vulnerability Statistics* [14];

2. To assist companies involved in software development and update to increase their solutions security level by *Enterprise Application Systems Development Issues* subproject [15];

3. To develop shareware tools for the enterprise application system vulnerability assessment by the *Enterprise Application Security Software* subproject ;

4. To assist companies in vulnerability assessment of the enterprise application system upon their implementation by the *Enterprise Application Systems Vulnerability Assessment Guide subproject* [17];

This report includes description and contents of the **Enterprise Application Systems Vulnerability Assessment Guide** subproject, where we describe vulnerability assessment scopes of enterprise applications and ERP systems.

Here are the general security domains of business applications:

• Network security;

• OS security;

• DBMS security;

• *Application security;*

• Front-end (client-side) security.

Due to unique character of application security, this document focuses on this issue only, while information about other layers you can find in eas-sec.org website [9].

General information

The Enterprise Resource Planning (ERP) systems such as the SAP allow to add some positive quality changes to information processing within an organization. However, while the ERP applications may solve some principal problems, they also may incur new associated risks. That is why the security is the most important aspect on the enterprise application and ERP system implementation.

"The Enterprise Application System Vulnerability Assessment Guide" describes 9 most known business application security issues relating to implementation and operation (the **Top 9 implementation issues**). This top issues list was prepared by the authors during vulnerability assessments of multiple business applications; this list may be applied to any of them. These issues are weighty factors for many emerging threats and related attacks. Prevention of these issues means getting ready to prevent numerous attacks targeted at business application security.

This document contains a detailed analysis of the most widespread business application platform - the **SAP NetWeaver ABAP**. During this analysis 33 key settings were identified and distributed between 9 issues mentioned above (the **Top 9 Implementation issues**). This guide show how to protect against te most widespread vulnerabilities in this area as well as provide further steps on securing all 9 areas .

The top-9 critical issues for business applications

Below, you can find the list of Top-9 critical issues for vulnerability assessment of business application. They are ranked from 1 to 9 according to their severity and impact on the ERP system, business applications and related security. For this list, 3 main parameters were considered:

1. initial access to exploit the vulnerability;

2. severity of vulnerability (a potential impact if exploited);

3. complexity of vulnerability exploitation.

This list is the same for all the business applications. In the next chapters, checks for each of these items (specific to the SAP NetWeaver ABAP platform) are described in detail. However, these description are stated in a way to ensure understanding of the basic principles relating to vulnerability assessment for any enterprise application systems.

Critical issue	Access	Severity	Simplicity
1. Patch management flaws	Anonymous	High	High
2. Default passwords for access to the application	Anonymous	High	High
3.Unnecessary functionality	Anonymous	High	High
4. Open remote management interfaces	Anonymous	High	Medium
5. Insecure settings	Anonymous	Medium	Medium
6. Unencrypted connections	Anonymous	Medium	Medium
7. Access control and SOD conflicts	User	High	Medium
8. Insecure trusted connections	User	High	High
9. Security events logging	Administrator	High	Medium

33 steps to securely configure the SAP NetWeaver ABAP

The Guide description

This section contains 33 steps to securely configure **SAP NetWeaver ABAP** platform, that were distributed among 9 issues mentioned above.

The authors' efforts were to make this list as brief as possible but also to cover the most critical threats for each issue. This approach is the main objective of this Guide: as despite best practices by the SAP, ISACA and DSAG, our intention was not to create just another list of issues with no explanation on why a particular issue was (not) included in the final list, but to prepare a document that may be easily used not only by SAP security experts. Report should also provide comprehensive coverage of all critical areas of SAP Security.

At the same time, the development of the most complete guide would be a never-ending story as at the time of writing there were more than 7000 checks of security configuration settings for the SAP platform as such, without those of specific role-based access and in-house applications.

As a result, each of the 9 issues includes major checks that must be implemented first and can be applied to any system regardless of its settings and custom parameters. It also important that these checks are equally applicable both to production systems and those of testing and development.

In addition to major all-purpose checks, each item contains a subsection called "*Further steps*". This subsection gives major guidelines and instructions on what should be done in the second and third place, and then how to further securely configure each particular item. The recommended guidelines are not always mandatory and sometimes depend on a specific SAP solution. On the one hand, with this approach, the authors were able to highlight key security parameters for a quick assessment of any SAP solution (from the ERP to the Solution Manager or Industry Solution) based on the NetWeaver ABAP platform and, on the other hand, to cover all issues and give complete recommendations on them.

In terms of quality, this makes the present Guide different from the SAP best practices that also contain few items, but do not cover the overall picture, as well as from best practices by ISACA and DSAG that have a lot of items, but the priorities are unclear and too complicated for the first step (though these papers are highly valuable and necessary).

33 steps to security

1. Patch management flaws

[EASAI-NA-01] Check for components update (SAP Notes)

[EASAI-NA-02] Check for kernel updates

2. Default passwords for access to the application

[EASAI-NA-03] Default password check for a SAP* user

[EASAI-NA-04] Default password check for the DDIC user

[EASAI-NA-05] Default password check for the SAPCPIC user

[EASAI-NA-06] Default password check for the TMSADM user

[EASAI-NA-07] Default password check for the EARLYWATCH user

3. Unnecessary functionality

[EASAI-NA-08] Access to the RFC-function via the SOAP interface

[EASAI-NA-09] Access to the RFC-function via the form interface

[EASAI-NA-10] Access to the Exchange Infrastructure (XI) via the SOAP interface

4. Open remote management interfaces

[EASAI-NA-11] Unauthorized access to the SAPControl (SAP MMC) service functions

[EASAI-NA-12] Unauthorized access to the SAPHostControl service functions

[EASAI-NA-13] Unauthorized access to the Message Server service functions

[EASAI-NA-14] Unauthorized access to the Oracle DBMS

5. Insecure settings

[EASAI-NA-15] Minimal password length

[EASAI-NA-16] Number of invalid logon attempts before the user account lock out

[EASAI-NA-17] Password compliance with the security policies in place

[EASAI-NA-18] Access control settings for RFC-service (reginfo.dat)

[EASAI-NA-19] Access control settings for RFC-service (secinfo.dat)

6. Access control and SOD conflicts

[EASAI-NA-20] The check for SAP_ALL profile accounts

[EASAI-NA-21] The check for accounts that may start any programs

[EASAI-NA-22] The check for accounts that may modify USH02 table

[EASAI-NA-23] The check for accounts that may execute OS commands

[EASAI-NA-24] Check for disabled authorizations

7. Unencrypted connections

[EASAI-NA-25] The SSL encryption to protect HTTP connections

[EASAI-NA-26] The SNC encryption to protect the SAP GUI client connections

[EASAI-NA-27] The SNC encryption to protect RFC connections between systems

8. Insecure trusted connections

[EASAI-NA-28] RFC connections that store user authentication data

[EASAI-NA-29] Trusted systems with low security level

9. Logging of security events

[EASAI-NA-30] Logging of security events

[EASAI-NA-31] Logging of HTTP requests

[EASAI-NA-32] Logging of table changes

[EASAI-NA-33] Logging of SAP Gateway activities

A detailed guide

1. Patch management flaws

The prompt installation of security support packages is one of the most important part in ensuring a full-scale system security. By the beginning of 2014, the SAP has released more than 2700 SAP Security Notes (to fix one or more vulnerabilities). Besides, on the second Tuesday of each month the SAP issues about 50 new SAP Security Notes of various severity levels. Some of those discovered by third-party researchers are included into a monthly acknowledgements with a direct reference to the issued SAP Note and to the researcher [18]. Prompt vulnerability elimination is necessary as the information on how to exploit them may get freely accessible and be implemented in such utilities as Metasploit. The number of support packages necessary for a system may be huge. That is why it is necessary to develop and establish a patch management process to ensure the implementation of adequate preventive measures against potential threats. Below, two major checks are given that must be in place to address the most critical problems

Further steps

It is also necessary to verify the security of the SAP components that are installed separately from the application server. These are services as SAP Router, SAP Webdispatcher, SAP GUI, and systems that are linked to the NetWeaver ABAP application server, but operate on the basis of the NetWeaver J2EE or SAP BusinessObjects application servers, with their security regulated by a separate document included in the EAS-SEC. In addition, a security patch should be checked for operating systems where the SAP services are installed, as well as for DBMS that store the SAP solution data .

- ***[EASAI-NA-01] Check for components update (SAP Notes)***

Description

Patches are designed to fix system errors by replacing the objects with outdated and vulnerable versions. There are two ways to fix a vulnerability: — to install the Support Package or — to implement the correction instructions from the SAP Notes. As a rule, initially a particular SAP Note (with appropriate correction instructions) is issued, then comes the Support Package, which includes, in addition to changed or new functionality, a set of correction instructions for a certain period of time.
As mentioned above, the number of support packages and SAP Notes required by the system may be huge. That's why the development of the patch management process should consider the patch installation priority based on the factors as follows:
— threat severity,
— threat probability,
— required system privileges,
— complexity of exploitation, and
— public exploit availability.

Attention! *The vulnerability management is additionally complicated by vulnerabilities that may be fixed with either a support package, or the SAP Notes. But these two mechanisms are not synchronized with each other, and this creates vulnerability management problems, e.g. a vulnerability fixed with a support package would not be implemented as fixed via the SNOTE transaction to the SAP Notes list.*

Threat

The issue of new security patches is linked to an identified vulnerability that rather quickly becomes publicly known (its description becomes freely accessible). A late implementation of security patches to fix certain vulnerabilities enables an adversary to exploit them, to get an unauthorized access to sensitive business data, to modify data and to perform a DoS attack.

Solution

It is necessary to perform regular checks for security patches implementation by following the main patch management process steps (data collection, risk assessment, implementing security patch software, result monitoring).
Technically, for the patch installation in 3.0 and higher versions, the SAP offers a tool known as the **SAP Patch Manager (SPAM)** (to start the SPAM, you can enter SPAM in the transaction code field) that allows to download and implement required support packages from the **On-line Server System (OSS)**. Besides, a the multi-purpose **SAP Software Update Manager (SUM)** may be used to implement various system update processes (note: a demo version is publicly available). [19]
To implement SAP Notes, use the **SNOTE** transaction to get a list of security notes required for particular system.
As mentioned above, these two mechanisms are not synchronized, so it can be improved manually or with some additional third-party tools.

- ***[EASAI-NA-02] Check for kernel updates***

Description

The SAP system kernel includes executables of the SAP Dispatcher, SAP Gateway, SAP Message Server, SAP Router and of other SAP main services . That is why the kernel has a separate update mechanism which is different from that of components. Kernel updates are released as service packs for a specific kernel type. Often, every next following support package is cumulative, i.e. with all previous updates, but sometimes releases contain updates for a certain support package only.

Threat

The issue of new security patches is linked to an identified vulnerability that rather quickly becomes publicly known (its description becomes freely accessible). A late implementation of security patches to fix certain vulnerabilities enables an adversary to exploit them, to get an unauthorized access to sensitive business data, to modify data and to perform a DoS attack.

Notice that kernel updates mostly fix highly critical vulnerabilities, as any system has a kernel. Thus, the priority of kernel update should be higher than that of components.

Solution

It is necessary to perform regular checks for security patches implementation by following the main patch management process steps (data collection, risk assessment, implementing security patch software, result monitoring).
For information on the current service pack via the SAP GUI: open the *Status* window in *System* tab and click on the *Other kernel info* (Shift+F5 by default). The information on the latest service pack is stored at the SAP support portal [20].
A SAP Note is usually downloaded as a system and executable files directory that replaces the previous files. The **Software Update Manager (SUM)** utility is also available to facilitate the manual process a lot (ref. to the operating manual [21]).

2. Default passwords for access to the application

Default passwords are one of the most common and frequently exploited software vulnerabilities, mainly due to low knowledge requirements and almost absolute efficiency. After installation, a SAP system has several standard clients: 000, 001, 066. These clients have default users with high privilege level by default (mostly the SAP_ALL profile). Besides, when new clients are created, they are created with default users and passwords.
On installation of SAP Web Application Server 6.10 and higher, the SAP* and DDIC user passwords are given as "Master Password" [22].
Vendor's default accounts and their passwords are well-known. They are given in the table below:

USER	PASSWORD	Client
SAP*	06071992, PASS	000, 001, 066, Custom
DDIC	19920706	000, 001, Custom
TMSADM	PASSWORD, $1Pawd2&	000
SAPCPIC	ADMIN	000, 001
EARLYWATCH	SUPPORT	066

Further steps

Some additional SAP components also have their own default passwords, e.g the SAP SDM and SAP ITS services of the old system versions have their own default passwords.
After the check for default passwords, a user password dictionary check should be run. To do this, it is recommended to use password brute force utilities, e.g., the John The Ripper.
In addition, the default passwords should be checked in all associated systems, such as network equipment, operating systems and DBMS that store the SAP system data . For example, an Oracle DBMS contains a lot of default passwords, including those specific for the SAP systems.

- ***[EASAI-NA-03] Default password check for a SAP* user***

Description

The SAP* user is created in all clients immediately after installation, it is a *dialog* user, i.e. a user type that enters and performs any actions in the system via the SAP GUI. This user is intended to copy clients, perform the license installation/renewal and other administrative tasks. The **SAP_ALL** profile is defined for it. If the SAP* user is removed, it is possible after system reboot to logon with a standard **PASS** password with the corresponding SAP_ALL privileges.

Threat

The default passwords of the **SAP*** user are well-known (see the table above). With these passwords, an adversary may enter the system with the **SAP_ALL** profile and, as a result, get an unlimited access to sensitive business data located in the system.

Solution

- Determine a new super user and lock the SAP* user out (but do not remove!) in all clients — go to SU01 transaction, select the SAP* user there and click on the Lock/Unlock icon (Ctrl+F5);
- Set **login/no_automatic_user_sapstar** (available in the **RZ10** and **RZ11** transactions) to **1**. In *3.1G and lower versions*, the *login/no_automatic_user_sap** parameter was used (with no effect to higher versions) (see the SAP Note 68048);
- Change the SAP* default password (using the **SU01** transaction);
- Ensure that the user belongs to the *SUPER* group in all clients (go to *SU01* transaction, select the *SAP** user, click on the *Change* icon (Shift+F6), then on the *Logon Data* tab.

- ***[EASAI-NA-04] Default password check for the DDIC user***

Description

The **DDIC** user is created in the 000 and 001 clients upon their installation (and copying). This default system user is intended for system installation, renewal, configuration and operation (implementation of support packages, Upgrade and Background job runtime of Transport Tool background jobs triggered by tp tool.). It is a dialog type user (may enter the system via the SAP GUI and perform any actions) in the 000 client; in all other clients it may be a *system* type user, that may perform background processing and interaction with the system. The **SAP_ALL** and **SAP_NEW** profiles that grant access to all SAP functionality are defined for this user.

Threat

The **DDIC** user default password is well-known (see the table above). With this password, an adversary may enter the system with the **SAP_ALL** (or SAP_NEW) profile and, as a result, get an unlimited access to sensitive business data located in the system.

Solution

Attention! *Do not remove the DDIC user or its profile! The DDIC user is necessary to perform certain tasks on installation, update, software delivery, and for the ABAP dictionary. The DDIC user removal results in a loss of functionality in these areas. But it is admitted (and recommended by some sources) to remove it in all clients except 000.*

- In 000 client change the user type to the **SYSTEM**;
- Remove the SAP_ALL profile;
- Lock out the DDIC user. Unlock it if needed only. Notice that the transport system executes certain programs on behalf of the DDIC user;
- Change the default password for the DDIC user;
- Ensure that the DDIC user belongs to the *SUPER* group in all clients to ensure that only authorized administrators may modify this account.
- Perform a regular check for system clients to identify rogue clients.

- ***[EASAI-NA-05] Default password check for the SAPCPIC user***

Description

The **SAPCPIC** user was intended for transports in the SAP solutions (in 4.5A and lower versions). It is a communication type user that may transport without dialog boxes for external RFC calls and is used especially for EDI (Electronic Data Interchange). This user does not have a dialog type user privileges, though it has the S_A.CPIC profile and, as a result, critical authorization objects as follows:
— the S_CPIC (to call for CPIC functions from the ABAP/4 programs),
— S_DATASET (with privileges to access files from the ABAP/4 programs), and
— S_RFC (authorization check for RFC access to the program modules, for example, a functional group).

Threat

The default password of **SAPCPIC** user is well-known (see above). With this password, an adversary can remotely execute RFC requests (e.g. to start some OS programs), execute arbitrary OS commands through RFC vulnerabilities (e.g. TH_GREP), create a dialog user with any privileges to enter the system and get an unlimited access to the sensitive business data in the system.

Solution

Remove the **SAPCPIC** user if you do not need it. If the user is necessary:
- Change the default password for the SAPCPIC user;
- Lock out the SAPCPIC user. Unlock if necessary only;
- If this user is required for EDI purposes (e.g. by contractor), never transmit this password via a remote session, use rather a separate communication channel, e.g. e-mail. Change the password immediately after the remote session is over;
- Ensure that this user belongs to the **SUPER** group in all clients to be sure that only authorized administrators may change this user account;

- Determine a special user for the remote access. Do not use any of default users;
- Perform a regular check for your clients to eliminate rogue clients.

- ***[EASAI-NA-06] Default password check for the TMSADM user***

Description

The **TMSADM** user is intended for transfers in the transport system. It is created automatically upon configuration and changes of **Transport Management System (TMS)** via the 000 client. It is a communication user, i.e. a user intended to transport without dialog boxes for the external RFC calls. It has the assigned **S_A.TMSADM** authorization profile enabled to utilize RFC-functions with GUI and to write to a file system. The **SAP_ALL** profile is also often assigned to this user.

Threat

The default password of **TMSADM** user default password is well-known (see the table above). An adversary may remotely start the RFC requests to perform critical actions such as deletion and reading files (EPS_DELETE_FILE, EPS_OPEN_FILE2), arbitrary ABAP code execution (through the RFC_ABAP_INSTALL_AND_RUN or TMS_CI_START_SERVICE function vulnerabilities), and, using the BAPI_USER_CREATE1 and SUSR_RFC_USER_INTERFACE requests, to create a dialog user with any privileges in a system and, as a result, to enter the system and get an unlimited access to the sensitive business data located in the system.

Solution

- Change the default password of TMSADM user; to change this password (according to Note 1414256 [24]) you should:

1. Enter the 000 client under any user with administrative privileges.
2. Start the **TMS_UPDATE_PWD_OF_TMSADM** program with the ABAP editor (the **SE38** transaction). You will find three options for the TMSADM password change:
— to enter your own password,
— to set a new standard password (according to the Note 761637 , *$1Pawd2&*), or
— to set an old standard password (PASSWORD);
3. Select the option *"To enter your own password'* on the appeared dialog box and enter the new password;
4. Start this program.

- Ensure that this user belongs to the **SUPER** group in all clients to be sure that only authorized administrators may change this user account;
- Determine a special user for the remote access. Do not use any of default users;
- Perform a regular check for your clients to eliminate rogue clients.

- Additionnally it is better to apply security notes releted to vulnerabilities in Programs which TMSADM user can execute such as:

- security note 1298160 for vulnerabilities TMS_CI_START_SERVICE.
- security note 1330776 for vulnerabilities in EPS_DELETE_FILE and EPS_OPEN_FILE2.

- ***[EASAI-NA-07] Default password check for the EARLYWATCH user***

Description

The EarlyWatch user is created in the **066** client upon SAP installation and is a dialog type user (that may enter via the SAP GUI and perform any actions in the system). It can be used for the SAP distance management and for access to the data on monitoring and efficiency. As a rule, it is used by the SAP AG customer support to access the customer's system and analyse problems (especially efficiency problems). Change the default password for EarlyWatch user, but **never remove** this user.

Threat

The default password for **EarlyWatch** user is well-known (see the table above). With this password, an adversary can enter the system with the **S_TOOLS_EX_A** profile and, as a result, perform various critical actions (for example, access any files, view sensitive tables or display external statistics records via the control tools). In old versions - 6.4 and lower, the user could execute critical transactions such as SE37 (function modules execution) and SE38 (running reports). In newer versions, it has less privileges, but it can exploit some vulnerabilities, e.g., the TH_GREP call with the SM51 transaction and, as a result, execute arbitrary OS commands.

Solution

Attention! Do not remove the Earlywatch user or its profile!
- Lock out the EARLYWATCH user. Unlock if necessary only;
- Change the default password for the **EARLYWATCH** user;
- Ensure that this user belongs to the **SUPER** group in all clients to be sure that only authorized administrators may change this user account;
- Perform a regular check for your clients to eliminate rogue clients.

3. Unnecessary functionality

Any more or less complex application has a large functionality that is necessary in general, but unnecessary for particular cases. This is highly important as almost all this functionality is enabled/activated by default (though with every next following version the security is getting higher: the extra functionality is disabled by default).
Often, the unnecessary functionality is misconfigured and performs critical actions in the system. Besides, the more functionality is available, the higher is the probability of vulnerabilities. Generally, the two locations of unnecessary functionality are web-applications and internal system objects (such as programs, transactions, RFC, etc.).
This section contains only checks for web-applications, as they can often be available via the Internet to the low-privileged or even anonymous users. The access to web-applications is implemented via the Internet Communication Framework (ICF) – the SAP Web Application Server component that enables to use standard protocols (HTTP, HTTPS and SMTP) for intersystem connections management through Internet.

Further steps

A standard installation contains about 1500 various web-services that are available remotely on behalf of any registered user, if the service is enabled by default. Besides, about 40 services are accessible to anonymous users. Immediately after three checks mentioned below, disable all services accessible to anonymous users, analyse which of the installed services you need, and additionally restrict the access to them with authorizations. The paper 'Secure Configuration of the SAP NetWeaver Application Server Using ABAP' [26], indicated 13 critical services. As mentioned above, these are only basic services.
*Another step after the Web-service configuration is disabling unnecessary internal functionality, such as unnecessary critical transactions, programs, profiles, roles, etc. This step requires a careful analysis of each module in each particular case. However, there is a range of transactions (*1 see the paragraph end) that are recommended to be disabled in the productive system in any case, which is mentioned in the ISACA guide ; this item is only a recommendation and wasn't included in the main list, as it is applicable to production systems only.*
****1 Transactions to be blocked (disabled):***
archive administration: KA10, KA12, KA16, KA18, SARA;
reset transaction data: OBR1;
structural authorization OICP, OOSB;
user maintenance: OMDL, OMEH, OMWF, OOUS, OPF0, OTZ1, OY27, OY28, OY29, OY30;
profiles: OMEI, OMWG, OOPR, OP15, OPE9, OTZ2, OY21;
privilege and profile maintenance: OMG7, OMWK, OPF1, OTZ3, OY20;
structural authorization: OOSP;
maintenance of user profiles: OVZ6;
copy by transport request: SCC1;
deleting a client: SCC5;
transport organizer (extended): SE01;
workbench organizer: SE09, SE10;
table maintenance: SE16, SM30, SM31;
external OS commands: SM49, SM69;
deleting all users: SU12.

- ***[EASAI-NA-08] Access to the RFC-function via the SOAP interface***

Description

A service at **/sap/bc/soap/rfc** is the SOAP interface to access RFC-functions (also known as function modules). With this service enabled and sufficient privileges, a legitimate system user and default user with default password may access and execute RFC-functions of the ABAP platform.

Threat

An undesired execution of an RFC-function may be started with the SOAP requests sent via the HTTP channel, in many cases, even from the Internet. An adversary can exploit default credentials to access the enabled RFC service and attack on anything, from regular access to non-critical information and

administrative system access. Also, a regular user with any set of privileges can perform a DoS attack with an incorrect SOAP request.

Solution

While using the /sap/bc/soap/rfc service, existing user authorizations to access it are recommended to be checked for adequate restriction. If the service is not required, disable it with the **SICF** transaction.

- ***[EASAI-NA-09] Access to the RFC-function via the form interface***

Description

The service available at **/sap/bc/FormToRfc** is intended for internal needs of SAP solution only and should not be located in the production system. This service lacks some authorization checks. In 6.20 and higher versions, this service was replaced by the SOAP service (/sap/bc/soap/rfc) to perform its functions, with the ICF services disabled by default.

Threat

There is a high risk with /sap/bc/FormToRfc service in the production system, as it lacks some authorization checks. An adversary may exploit this vulnerability to attack via the RFC-function call, and, as a result, to get an unauthorized access to the sensitive business data.

Solution

It is recommended to disable the **/sap/bc/FormToRfc** service with the **SICF** transaction if it is not used.

- ***[EASAI-NA-10] Access to the Exchange Infrastructure (XI) via the SOAP interface***

Description

This service is the SOAP interface to access the Exchange Infrastructure (XI). With this service, an adversary may remotely call critical functions and - much more important - send requests to third-party systems accessible by this service.

Threat

An undesired execution of an XI-function with the SOAP requests via the HTTP channel is possible if this service was activated incorrectly or the restrictions for the authorization are insufficient. An adversary may exploit default credentials to access this service. In this case, there is a risk of attack both of the target system and of those integrated ones, depending on the functionality in the Enterprise Service Bus. At worst, unlimited access to this server and other infrastructure services is possible.

Solution

It is recommended to disable this service with the SICF transaction. If this service is required for business purposes, you should restrict the access with appropriate authorizations and network access control.

4. Open remote management interfaces

The SAP NetWeaver platform is not only the Dispatcher service that is responsible for user connections by the SAP GUI, but also a whole range of another services, with each of them listening to a remote port and accepting network connections. Some of these services grant administrative access and remote administration functions, as well as an access to various technical services such as a load balancing system of the SAP Message Server or a remote administration system of the SAP Management console.

These services can be available for connection from the corporate intranet or the Internet and have insecure settings that allow to manage them remotely without authentication data. This section contains the most insecure services, which functionality should not be accessible from the corporate intranet.

Further steps

Except those mentioned above, the system has other less critical and widespread services (e.g. the Message Server HTTP). But you should restrict access to them as well. For a full list of the SAP services refer to paper "TCP/IP Ports Used by SAP Applications". This list also depends on the components that are used in each particular system.
Besides, consider third-party services that may be enabled on this server, such as remote administration interfaces for various DBMS, remote monitoring and data backup systems, etc., the access to which must be restricted using authentication both at the network and application levels , if possible.

• *[EASAI-NA-11] Unauthorized access to the SAPControl (SAP MMC) service functions*

Description

The SAP Start Service starts on every computer along with the SAP solution instance. In Windows, this process is executed with sapstartsrv.exe, in UNIX - with sapstartsrv. The SAP Start Service provides the following functions for the SAP solution, instance and process monitoring:
- start and stop;
- monitoring the active state;
- reading logs, trace files and configuration files;
- technical information, for example, on network ports, active sessions, etc.

These services are provided in the **SAPControl SOAP Web Service** and are used by the SAP monitoring tools *(SAP Management Console, NetWeaver Administrator* and others).
While service runs, it uses the following ports:

- HTTP port **5<xx>13** (or *sapctrl<xx>* in /etc/services), where <xx> is the instance number;
- HTTPS port **5<xx>14** (or *sapctrls<xx>* in /etc/services), where <xx> is the instance number.
the HTTP port 50013 or the HTTPS port 50014 are used for 00 instance. [29]
This process allows to read various system information without user's consent. However, it requires user authentication for secure operations such as the SAP instance start and stop. The sapstartsrv controls the internal secure operation list (with default operations depending on release). It can be changed if required using the start profile parameter **service/protectedwebmethods**.

Threat

Many insecure methods enable getting information on the system configuration or status and remote retrieval of all system parameter settings, read the log and trace files that may contain user passwords or HTTP session files. This information may be used to develop more critical attacks.

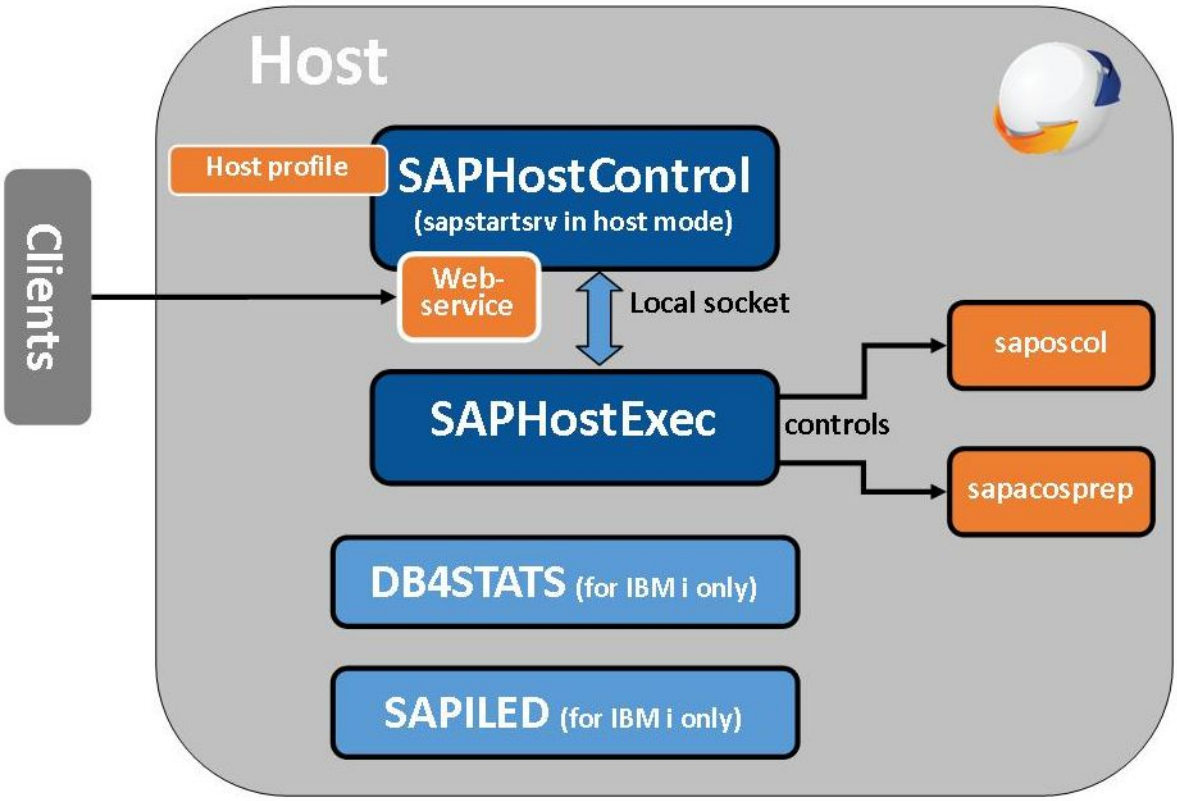
Solution

As mentioned in SAP Note 1600846[30], the **sapstartsrv** must be reconfigured by setting the **service/protectedwebmethods** parameter to ***DEFAULT*** in a default system profile (*DEFAULT.PFL*). Then, all sapstartsrv services should be restarted in the cluster to activate changes. This value implies a default list of all critical methods. You can also use the ALL value (i.e. all methods), though it is considered excessive to some extent (the parameter and its values are described in detail in SAP Note 927637 [31]).
Implementation of SAP Note 1439348 may be seen as an additional patch for this vulnerability, and the recommendations presented there may also be used.
We recommend to restrict access to this service by IP-address; thus, to define the Access Control Lists (ACL) and change values for services/http/acl_file and /https/acl_file.

- ***[EASAI-NA-12] Unauthorized access to the SAPHostControl service functions***

Description

The **SAP Host Agent** is a component for other various components management, control and monitoring, which consists of the following services and programs:
- the **SAPHostExec**, which is a control program started by *root* (UNIX) or *LocalSystem* (Windows) accounts. It controls all functions required by these specific users, e.g., the OS saposcol and sapacosprep collectors. The program is connected with the sapstartsrv in a host mode (see the picture) via the local socket that provides high-speed and secure connection and starts upon the host start as well.
- DB4STATS and SAPILED are programs that provide the SAP Database Performance Collector and the SAP ILE daemon for the IBM I respectively.



- **SAPHostControl** (*sapstartsrv* in the host mode) is the SAP NetWeaver management agent, that is an executable of *sapstartsrv*, run in the host mode by the *sapadm* user and utilizes the remote **TCP 1128** port. That is why it is responsible not for the SAP instance but for any monitoring on the host that is centrally controlled.
A profile used upon the start of executable files determines the sapstartsrv operating mode: instance (with an appropriate instance profile) or host (with the host's own profile that may include parameters ***SAPSystem* = 99**, ***SAPSystemName* = SAP**). [33]
For data transmission, the **SOAP** protocol is utilized which is encapsulated into the **SSL**, if encryption is in place. This service allows to read some system information without user consent and has vulnerabilities to start the remote OS commands.

Threat

The SAP Netweaver enables a remotely authorized adversary to execute an arbitrary code in the system due to the SAPHostControl service maintenance error, if this service does not properly validate the incoming data to the SOAP management interface. With the SOAP interface running on TCP port 1128, an adversary can exploit this vulnerability to inject and execute arbitrary commands in the system with the administrative privileges.

Many insecure methods enable to request the information on the system configuration or status, to read log and trace files that may contain user passwords or the HTTP session files and to remotely execute OS commands through the OS command injection vulnerability (see SAP Note 1341333 [34]). This information may be used to develop more critical attacks.

Solution

For this service, the vulnerability to remotely execute an arbitrary code by an OS command injection was fixed in May 2012 with SAP Security Note 1341333 [34]. To avoid information disclosure, SAP Security Note 1816536 [35] was released in April 2012. Both of these SAP Notes are functional and sufficient to fix the vulnerabilities.
For more security, the access control by the IP address should be restricted to this service by a personal firewall or, in case of network equipment, by granting access to required data servers only.

- ***[EASAI-NA-13] Unauthorized access to the Message Server service functions***

Description

The SAP Message Server is a system component that, on the one hand, controls the communication between application servers (dialog instances) of one SAP system and, on the other hand, ensures the load balancing from clients such as the SAP GUI.
With the standard installation of 7.0 and lower versions, both clients and application servers use the Message Server port for interaction. In 7.0 and higher versions, with the default installation the Message Server port is automatically segregated into an internal port (used for application connections to the server) and an external port (used for the end user connections).
If activated, the Message Server ACL can control the addresses of possible connections. For this effect, use the **ms/acl_info** parameter indicating a file with Message Server access configuration, that contains application server's host and domain names, IP addresses and/or subnet masks that the Message Server can accept. External clients are not affected upon information retrieval from the Message Server (always accessible). The default parameter value: */usr/sap/<SID>/SYS/global/ms_acl_info*.

Threat

Without ACL file or its misconfiguration, a malicious software or potential adversaries may get an access to the Message Server and register their own application server to perform a "man-in-the-middle" attack and to intercept the credentials of legitimate users that attempt to connect to the Message Server. This can result in access to user accounts.

Solution

Set up the **ms/acl_info** parameter indicating the ACL file for the Message Server (default value = */usr/sap/<SID>/SYS/global/ms_acl_info).* This file should contain the application servers' host and domain names, IP addresses and/or subnet masks acceptable by the Message Server with the following syntax:

*HOST = [*| ip | hostname | network mask | domain] [, ...]*
The configuration file allows to use the "*" wildcard in access control description (e.g., HOST = *.sap.com or HOST = 157.23.45.*). The "*" wildcard should be avoided, particularly in "HOST = *", as it enables access from any workstation.
The access control settings do not affect retrievals of technical information from the Message Server (always accessible).

Alternatively, follow these recommendations:
- In 4.5 and lower releases, the Message Server port defined in parameters (**rdisp/mshost, rdisp/msserv**) should override the firewall settings. The access to this port should be granted to network segments with SAP servers only.
- For 6.4 and lower releases, the server services should be distributed between two ports - one for the SAP GUI client access (**rdisp/msserv**), the other - for access to internal connections with the server (**rdisp/msserv_internal**).

- ***[EASAI-NA-14] Unauthorized access to the Oracle DBMS***

Description

Currently, the Oracle DBMS is the most widely used DBMS along with the SAP. Unfortunately, this DBMS if installed with the SAP has an insecure **REMOTE_OS_AUTHENT** configuration for the trusted operations between SAP solutions and is able to circumvent security controls like DBMS password.
The only way to mitigate this risk is to restrict remote access to the port of Oracle DBMS for IP addresses of necessary servers only.
This setting is implemented using the **Sqlnet.ora** configuration file. The **tcp.validnode_checking** parameter discussed here is required for the host names validation upon their attempts to establish inbound connections. With the *yes* value of this parameter, the inbound connections are checked against nodes listed in TCP.INVITED_NODES or TCP.EXCLUDED_NODE (while the first one is of higher priority). The TCP.INVITED_NODES, in turn, requires each client host to be included in the sqlnet.invited_nodes server list.

Threat

If there are no restrictions for the client nodes, an attacker can connect to the Oracle DBMS without the password, using a trusted login **$OPS<SID>adm**, that will allow it to get nearly full access to the DBMS.
One more (next) step is to decrypt the **SAPR3** user password from the **SAPUSER** table and to connect to the DBMS with its privileges. This user has a full access to the SAP data, thus an adversary can get an unlimited control over the system.

Solution

Set the **tcp.validnode_checking** parameter in the **sqlnet.ora** file to "*yes*" so that the inbound connections are checked against the **sqlnet.invited_nodes**, i.e. a list of permitted hosts. Obviously,

you should specify all client hosts in the sqlnet.invited_nodes server list that are allowed to establish inbound connections. It is recommended to limit this list by trusted systems only.

5. Insecure settings

Though not included in the mentioned issues, some security settings of any application are also critical. Among these settings we can mention both the standard settings (password length and complexity, number of invalid password attempts) and more specific ones for each given system. In this case we outlined the SAP Gateway service access settings.

Further steps

The number of various fine-tuned security settings is enormous, and there are specific ones for each particular SAP solution or module. Start with the document called SAP NetWeaver Security Guide, the User Authentication section, then, you may examine the documents on particular services and modules security configuration [36] in detail.

- ***[EASAI-NA-15] Minimal password length***

Description

Choosing a user password, consider that passwords should meet some internal requirements established by the SAP system and corporate policies. There are various profile parameters that are to control the compliance to these requirements. One of these basic parameters is **login/min_password_lng**, which specifies the minimal password length allowed for account protection. A value defined in this parameter by default is **6**, acceptable values are: **3 - 40**.

Threat

If the defined minimal password length is **less than 8 characters**, an adversary may easily brute force passwords with knowing a hash from the **USR02** table or run remote brute force, if the **login/fails_to_user_lock** parameter (defines the number of invalid logon attempts before the user is locked out by the system) is set incorrectly.

Solution

Set the **login/min_password_lng** parameter value not **less than 8** (or as defined by the company security policy) to mitigate the risk of potential password attack.

- ***[EASAI-NA-16] Number of invalid logon attempts before the user account lock out***

Description

The **login/fails_to_user_lock** parameter defines the maximum number of invalid password attempts before the user account is locked out. It is important because it interacts directly with the

login/min_password_lng parameter that defines the minimum password length allowed and prevents a remote password brute force attack. A value defined in this parameter by default is **5**, acceptable values are: **1 - 99**.

Threat

If the **login/fails_to_user_lock** parameter is set incorrectly or has a low value, an adversary may succeed in carrying out a brute force attack and get an unauthorized access to user credentials.

Solution

Set the **login/fails_to_user_lock** parameter value **not more than 6** to mitigate the risk of potential brute force attack.

- ***[EASAI-NA-17] Password compliance with the security policies in place***

Description

The **login/password_compliance_to_current_policy** parameter is highly important as, with no such parameter or zero value, the password length and complexity settings will not automatically apply to old users (but to newly created only). Thus, all old users may have insecure passwords. If this parameter is set to 1, the policy is applied to old users that use insecure passwords and forces them to choose secure ones on logging into system.

Threat

If the **login/password_compliance_to_current_policy** parameter is set to "0", the password policy compliance for old users is not set. This allows users to have passwords that are not compliant with the security policies and, as a result, these user accounts may be easily compromised.

Solution

Set the **login/compliance_to_current_policy** parameter to "1" to apply the password policy requirements for all users, including those newly created.

- ***[EASAI-NA-18] Access control settings for RFC-service (reginfo.dat)***

Description

The **SAP Gateway** is the application server technical component to manage communications between SAP systems for all RFC-based functionality. Since the gateway is an application server interface for external connections (with other SAP systems, external programs, etc.), higher security requirements are applied. The SAP Gateway security is controlled by the **reginfo** (defined by the **gw/reg_info** parameter) and the **sec_info** files (defined by the **gw/sec_info** parameter).

Some clients may be allowed to register their services on the server. Specify the services registered in the **reginfo** file to control the access to them, cancel their registration, determine external server services allowed to be registered on the gateway. The file name (file path) is defined by the **gw/reg_info** parameter. The default file path is: **/usr/sap/<SID>/<INSTANCE>/data/reginfo**.
If this file doesn't exists, any server processes may be registered from any hosts (notice that from 7.20 and higher kernel releases, for security purposes, this process is restricted by the gw/acl_mode instance profile parameter; see SAP Note 1480644 [37]), and if this file is empty or has no valid records, the registration is not allowed.
If someone is trying to register a service on the gateway, the valid record is looked up in the file, specifying this user right to register a particular service. If the record is not found, the registration is denied. It is important to understand that the reginfo file is read only ONCE, upon program registration. All further changes and restrictions in the reginfo file don't affect the successfully registered programs.

Threat

In case the **reginfo.dat** file is absent or its configuration is incorrect (for example, a wildcard "*" is used in host definitions), an adversary may register any service on the SAP Gateway and get an unauthorized access to the SAP server. Also, they may register a new service (with malicious functionality) under the same name as one already existed, thus raising a risk of its execution by legitimate users.

Solution

Unauthorized service registration may be avoided by creating a **reginfo.dat** file in the SAP Gateway data directory. If the file exists, the system checks this file against the access rights for the remote RFC program call, thus preventing an unauthorized access.
The file records should have the following syntax (where each line has a TP record and other optional parameters):

TP=name [NO=<n>] [HOST=<host>] [ACCESS=<host>] [CANCEL=<host>] , where:

TP=name is a registration ID of the external server program.
NO=n shows what number of registrations with that ID is allowed.
HOST=<host> is (a) name(s) of a host from which the registered servers may enter the system. Here you may specify the host names, IP addresses, domain names or subnet masks. The registration is allowed only if the server enters the system from this node. Without this optional parameter, the registration is allowed from any host.
ACCESS=<host> is host name(s) that is (are) allowed to use the registered service. Here you may specify the host names, IP addresses, domain names or subnet masks. The local system is always allowed to use the server. Without this optional parameter, the server may be used from any node.
CANCEL=<host> is (a) host name(s) that allow(s) to log off from the registered system server. The applied rules are the same as for the *ACCESS* parameter.
In 6.40, patch 212; 7.00, patch 139; 7.10, patch 80, and higher kernel versions, the syntax is added with the permit and deny values indicated by the Latin upper-case "P" and "D" respectively (see SAP Note

1105897 [38]). *"P"* permits program registration, (as in the old syntax line); *"D"* denies it. The first line layout in this file is **#VERSION=2**. All next lines are structured as follows:

P|D TP=name [NO=<n>] [HOST=<host>] [ACCESS=<host>] [CANCEL=<host>]

Attention: *the system reads the key words in the upper-case only. An incorrect specification - HOST=* wildcard – results in undesired accesses (fixed by correction instructions in SAP Note 1473017[39]). The key words should be separated with commas in all host name lists (HOST, ACCESS and CANCEL). Any space will indicate the end of host name list. A detailed explanation of this syntax is given in SAP Note 1069911 [40].For the correct reginfo.dat configuration use the SAP Note 1425765 u 1408081 recommendations. [41], [42]*

- ***[EASAI-NA-19] Access control settings for RFC-service (secinfo.dat)***

Description

In the **secinfo** file, you may specify external services that may be started, users allowed to start them, and external server services allowed to be registered on the gateway (in 46D and lower kernel releases only; in 6.40 and higher, the service registration from external servers is controlled with a separate RegInfo file). In other words, the secinfo security file is used to prevent unauthorized start of an external program.
The file name is defined by the parameter **gw/sec_info.** The default file path is: **/usr/sap/<SID>/<INSTANCE>/data/secinfo**.
Without this file, the system starts all external programs, and if this file is empty or has no valid lines, no external service may be started.
Upon start of an external service, the system checks the file for a valid record, and if this check fails, the system denies the external service start and shows an error message.

Threat

With no secinfo.dat file or its insecure configuration (e.g., with "*" wildcard in host, program of subnets definitions), an adversary may start a required service registered in the SAP Gateway, get an unauthorized access to its functionality, and, in some cases, to the SAP server, with the services executing OS commands.

Solution

Unauthorized programregistration may be prevented by creating a **secinfo.dat** file in the SAP Gateway data directory. If the file exists, the system checks this file against the access rights for the remote RFC program call, thus preventing an unauthorized access.
The syntax of the file records should be as follows (where USER, HOST and TP and other parameters in each line are optional):

TP=name HOST=<host> USER=<user> [USER-HOST=<user-host>] , where:

TP=<program name> is a name of a program to start (in addition, you can specify a wildcard for program ID, e.g., TP=XYZ*)

USER-HOST=<host> (in other words, a source address) is a user host name allowed to start a program. in the reg_info file syntax, this parameter specifies the client address; it is available from 6.40, the patch 194; 7.00, patch 119 and higher versions).
USER=<user> is a username allowed to start a program. If the program runs from the application server, this is a system username, and if the program is external, this is the OS username.
USER-HOST=<host> (in other words, a source address) is a user host name that may start the program. For security purposes, this option is strongly recommended (see SAP Note 1434117 [43]).
In 6.40 and lower versions, the PWD=<Password> parameter was supported (ignored in newer systems).
In 6.40, patch 212; 7.00, patch 139; 7.10, patch 80, and higher kernel versions, the syntax is added with the permit and deny values indicated by the Latin upper-case "P" and "D" respectively (see SAP Note 1105897 [38]). "P" permits start of the program (the same as the old syntax line); "D" denies it. The syntax of the first line in this file is **#VERSION=2**, and that of all next lines is:

P|D TP=<tp> HOST=<host> USER=<user> [USER-HOST=<user_host>]

Attention (!): *the system reads key words in the upper-case only. An incorrect specification results - the HOST=* wildcard – results in undesired accesses (fixed by the correction instructions in SAP Note 1473017[39]).*
A detailed explanation of this syntax is given in SAP Note 614971 [44].
For the correct secinfo.dat configuration refer to SAP Note 1408081, 1525125, 1425765. [42] [45] [41]

6. Access control and SOD conflicts

The SAP solution has a lot of various functional opportunities which are implemented through programs, transactions and reports. The access to these objects should be strictly regulated based on the authorization values defining users, methods and objects allowed for access. Access to critical actions (e.g., access rights to modify transactions or to read any tables) enables users to perform attcks on SAP systems, , escalate their privileges or to steal critical data.
Segregation of Duties (SoD) is a security method to prevent conflict of interests, i.e., to avoid two of more access rights which - being granted together - may give rise to a risk of fraudulent actions (e.g., a right to create and to approve a Payment Order). The SoD helps to segregate incompatible responsibilities that enable an individual to commit fraud.
This issue gives only 5 basic checks for this access control scope that cover the most critical access rights and relevant settings. Since the SoD is based on the business processes of an individual company (i.e., an individual method) and its configuration is the second step after assigning critical duties, we give no check for SoD in this issue.

Further steps

In the SAP BASIS only, there are about hundred of such critical privileges, with each module including a similar number. As mentioned above, sometimes these privileges overlap each other and that is under control of the SoD matrix. A standard matrix contains more than 200 different SoD patterns, while, depending on the functional area, each company can use their ones.

Besides, there are other critical access rights specified both in the ITAF regulatory document by the ISACA [46] and the DSAG [47] standard by the Deutschsprachige SAP Anwendergruppe. Then, go to the SoD configuration. Before the SoD analysis, you should check authorization values for wildcard "" in access rights. Often, these rights are excessive and cause hundreds of various SoD conflicts.*

- ***[EASAI-NA-20] The check for accounts with SAP_ALL profile***

Description

The **SAP_ALL** profile is a composite profile with all privileges for a SAP solution, including those for the main administrative and application settings. According to the SoD principle, this profile has no practical use.

Threat

A user that has the **SAP_ALL** profile may perform any actions in the system. If the SAP_ALL profile user authentication data was compromised, the adversary gets an unlimited access to the sensitive business data and processes.

Solution

- The user privileges should be specified according to the least-privileges principle.
- The **SAP_ALL** profile should be used in case of emergency only.
- You should create only one user with such a profile (for emergencies) and keep this user password in secret. Instead of the SAP_ALL profile, you should distribute its privileges to appropriate positions. You should assign, e.g., not all SAP_ALL privileges to a system administrator (or to a super user), but only relevant ones, i.e. S_* privileges. These authorizations will grant a system administrator enough privileges to administer the entire SAP solution, not allowing him to perform tasks in other areas, e.g., HR management.

- ***[EASAI-NA-21] The check for accounts that may start any programs***

Description

Any user with authorization to start a program may start any programs, if the additional access control inside some specific programs is not implemented, that is often met in practice, especially in the client programs. For the program access control, authorization groups are created. Several ABAP programs are defined for each authorization group. The users may start only those programs that are included in the authorization groups assigned to their profiles.
Check for users with the critical access privileges as follows:
The **SA38** transaction to execute programs and reports in the system;
The **SE38** transaction to see the source code of programs and to develop/debug them;
The **SE37** transaction to start function modules;
The **SE80** transaction to edit any objects under development (i.e. in ABAP editor).

Threat

Users enabled to execute any programs have an unlimited access to system functionality and may seriously damage the system, since there are more than 30K various programs to implement almost any action: from creating a user and executing OS commands to payments for the goods and salary modification.
With no control, any user with S_PROGRAM authorization object and access to SA38 or SE38 transactions may execute any program, with access to SE37 - start any function module, to SE80 - perform editing of any objects under development. The editing and start of some programs may create additional risk that the program may return the inaccurate or incomplete information. Besides, if a user may start SE38 transaction, it can lead to unauthorized program modification that can impact system integrity.

Solution

- Minimize the number of users with these privileges, roles should be assigned according to the least-privileges principle.
For access control over these transactions, monitor users with the following authorizations:
S_PROGRAM:P_ACTION=SUBMIT *or* ***BTCSUBMIT***
S_PROGRAM:P_GROUP=*
S_TCODE:TCD=SA38 *or* ***SE37*** *or* ***SE38*** *or* ***SE80***
- If possible, add more authorization checks to the most critical programs by their source code modification.
- Besides, perform a review of policies, procedures and criteria associated with authorization group specification for new programs.

- ***[EASAI-NA-22] The check for accounts with the privileges to modify sensitive tables with passwords***

Description

The USR02, USH02 and USRPWDHISTORY tables are the SAP-system standard tables that contain such sensitive user data as the user name, password hash, user type, client ID, etc.
For access control over these tables, the users with the following authorizations should be monitored:
For the SAP NetWeaver version with S_TABU_NAM authorization object support:
S_TABU_NAM*:ACTVT=02;*
S_TABU_NAM*:TABLE=****USR02*** *or* ***USH02*** *or* ***USRPWDHISTORY***
or (for all other version):
S_TABU_DIS:ACTVT=02;
S_TABU_DIS:DICBERCLS=SC.

Threat

The access to tables mentioned above enables users to change any user password hash and to enter the system under any account.

Solution

The number of users with access to the **USR02, USH02, USRPWDHISTORY** tables should be restricted on a business need basis. The roles should be assigned according to the least-privileges principle.

- ***[EASAI-NA-23] The check for accounts that may execute OS commands***

Description

For the SAP solution to interact with the host OS, some specific mechanisms are implemented for interaction with external OS commands. These OS commands may be executed with the transactions defined in the SAP solution and by users with specific privileges only.
The **SM49** transaction allows to execute any external commands (related to the OS). The SAP solution contains a detailed information for each external command, including directly the OS command, pre-defined parameters and the information whether the additional parameters are permitted.
The **S_LOG_COM** authorization object should be assigned to users executing external commands. The **S_LOGCOM_ALL** authorization object (based on S_LOG_COM) allows execution of any command included in the **S_A.SYSTEM** and **S_A.ADMIN** standard authorization profile sets.
To control external commands, the **SM69** transaction is used. It allows to modify them and to install additional security controls. The user should be granted with the **S_RZL_ADM** authorization object with Activity "**01**" in authorization profile.

Threat

The users that may execute or modify the OS commands have a potential opportunity to start critical OS commands and may seriously damage the system.
Without control, any user with access to **SM49** or **SM69** transactions (and access to **S_LOG_COM** or **S_RZL_ADM** authorization objects) may execute the command of OS that is external for a SAP solution. The editing and start of some programs may create additional risk that the command may return the inaccurate or incomplete information. Besides, the user authorization right to start the **SM69** transaction may result in unauthorized command modification that, in turn, may effect both the OS and SAP solution integrity.

Solution

- Minimize the number of users with these privileges, roles should be assigned according to the least-privileges principle.
- Block these transactions and unlock them if necessary during utilization.
- Besides, perform a review of policies, procedures and criteria associated with authorization group specification for new programs.

- ***[EASAI-NA-24] Check for disabled authorizations***

Description

The authorization checks are used each time when it is necessary to verify that the user has the appropriate rights to perform certain actions.
The checks of particular authorization values can be disabled at the system level. The check is not performed, if the administrator intentionally disables the check for authorization object for a particular transaction (with **SU24/SU25** transactions). This may be useful, as upon execution of transactions, often a lot of authorization objects are checked that are called by transaction in a background mode.
For successful checks, a user should have appropriate authorizations. In effect, some users are often given more authorizations than necessary. These authorizations along with some others may grant a user additional (extra) privileges and increase the workload.
On the other hand, a disabled authorization check may incur a high risk as it may disable the access control mechanisms of the system.
To put disabled authorizations in place with SU24/SU25 transactions, set the **AUTH/NO_CHECK_IN_SOME_CASES** profile parameter to **Y** (with **RZ10** transaction). This setting is used by default in newer version of BASIS. This parameter allows to disable the authorization check for individual transactions.

Threat

No critical authorization check gives rise to risk of some unauthorized critical actions in the system, loss of system capacity or committing fraud. Besides, such disabled authorization checks may indicate a backdoor in the system.

Solution

It is recommended to verify necessity of disabling of authorization check for system authorization object in a particular program, transaction or RFC-function. For this, analyse the names of programs, transactions or RFC-functions with system authorization objects where authorization check is disabled. Technically, disabled authorizations are marked in the **USOBX_C** table (a validation table for the **USOBT_C** table) with **OKFLAG = N** field value.
For some authorization objects in individual transactions, authorization checks should be disabled only for the period of their execution.

7. Unencrypted connections

To protect connections between the SAP NetWeaver system components, especially against the man-in-the-middle (MITM) attacks, it is necessary to ensure security at the transport level. When using the **Transport Layer Security (TLS)**, the data transmission may be protected from eavesdropping not only with encryption, but also with the partner authentication.
The TLS use ensures the following protection types:
- *Authentication:* Communication partners may go through authentication. The server is always authenticated, while the client is authenticated depending on the algorithm.
- *Data integrity:* The message exchange is protected so that any modification is revealed.

- Data confidentiality: the data transmitted between the client and the server is encrypted to ensure its confidentiality. The eavesdropper is not able to get access to the data. The protection is available for inbound and outbound connections.
The security is provided in two forms, depending on the used connection type. For connections using the Internet protocols such as the HTTP, the **Secure Sockets Layer (SSL)** protocol is used. For the SAP protocols such as the RFC, the **Secure Communications Network (SNC)** is used.

Further steps

This section contains the detailed encryption settings for various services. However, you should understand that, even if the encryption is enabled, it is not always securely configured: there are various fine-tuned setting protecting against attacks for each encryption type and for each particular case. For example, recent BEAST and CRIME attacks on the SSL determined the need for more SSL fine-tuned settings [48]. That is why you should configure the encryption very carefully, considering new attack types and specifics of the configured service.

- ***[EASAI-NA-25] The SSL encryption to protect HTTP connections***

Description

The SSL supports the following protocols:
— HTTPS from HTTP,
— IIOPSEC from the IIOP,
— P4SEC from the P4.
In this case, we consider HTTP only, as IIOP and P4 belong to the JAVA stack.
In the parameter **icm/server_port_<xx>** of the ICM service, the protocol and port are specified, where **<xx>** is the order number of parameter. This parameter is used to specify the service name or port number employed by the protocol. Also, additional service properties may be defined. But each port may not have more than one assigned service. Besides, the service can not start with another program already using this service or port.
The parameter line has the following syntax: ***PROT = <protocol name>, PORT = <port name> [, TIMEOUT = <timeout>, PROCTIMEOUT = <proctimeout>, EXTBIND = 1, HOST = <host name>, VCLIENT = <client SSL Verification>, SSLCONFIG =]***.
Mandatory parameters are a protocol name (PROT) and a service name or port number (PORT), other parameters are optional. The default values for this parameter depend on the system type specified by parameter **system/type**. The following types are available:
- The double stack: **system/type = DS** (currently out-of-date). The instance contains AS ABAP and Java AS application servers:
icm/server_port_0=PROT=HTTP,PORT=5$(SAPSYSTEM)00,TIMEOUT=60,PROCTIMEOUT=600
icm/server_port_1 = PROT=P4,PORT=5$(SAPSYSTEM)04
icm/server_port_2 = PROT=IIOP, PORT=5$(SAPSYSTEM)07
icm/server_port_3 = PROT=TELNET,PORT=5$(SAPSYSTEM)08,HOST=localhost
icm/server_port_4 = PROT=SMTP,PORT=0,TIMEOUT=120,PROCTIMEOUT=120

- the Java only: **system/type = J2EE** (not covered by this document). The instance contains the Java AS application server only.
- the ABAP only: **system/type = ABAP**. The instance contains the ABAP (AS ABAP) application server only.

icm/server_port_0 = PROT=HTTP,PORT=0,TIMEOUT=30,PROCTIMEOUT=60
icm/server_port_1 = PROT=SMTP,PORT=0,TIMEOUT=120,PROCTIMEOUT=120

Threat

No encryption of network connection may lead to interception of transmitted data, thus to an unauthorized access. The HTTP protocol transmits all authentication data as plain text, that allows to intercept it easily with the spoofing attack.

Solution

For HTTP connections, you should configure SSL. Detailed step-by-step instructions for this process may be found in the paper *SSL Configuration in SAP ABAP AS and JAVA AS – Step-by-step procedure* .

- ***[EASAI-NA-26] The SNC encryption use to protect the SAP GUI client connections***

Description

The **SNC** (Secure Network Communications) is a software layer in the SAP solution architecture to ensure secure interface for external products; particularly, it ensures encryption and authentication.
SAP solutions contain basic security controls including password-based user authorization and authentication concepts. With SNC in place, you may improve the SAP solution security by implementing additional security functions not directly provided by SAP solutions (e.g., use of smart cards for user authentication, additional digital and encryption certificates).
You may apply up to three security levels (parameter **snc/data_protection/use** is intended for this /default value is 3/ and ensures a standard level of connection security, it also has associated parameters **snc/data_protection/max** and **snc/data_protection/min** for the maximum and minimum security levels respectively):
- Authentication only (*snc/data_protection/use=1)*. The system authenticates the communication partners. It is the minimum security level provided by the SNC. A real data protection is not ensured!
- The integrity protection (*snc/data_protection/use=2)*. The system detects any data modifications (manipulations) that may occur between two communication endpoints.
- The data confidentiality protection (*snc/data_protection/use=3*). The message encryption system makes the eavesdropping useless. This level also includes the data integrity protection. It is the maximum security level provided by the SNC.

The **snc/enable** parameter defines whether the SNC protection is used for connections.

- The default value is: 0 (inactive SNC).
- The secure value: 1 (active SNC)

As soon as the SNC is active (snc/enable = 1), the system accepts the SNC-protected connections only. If there is a need to accept a normal connection which is not protected by the SNC, it is necessary to set the appropriate parameters (**snc/accept_insecure_gui, snc/accept_insecure_rfc,**

snc/accept_insecure_cpic) depending on the types of connections that needs to be insecurely accepted.

Threat

No SNC encryption may lead to unauthorized access to data transmitted between the systems using **DIAG** and **RFC** protocols. These protocols employ insecure compression algorithms only instead of data and password encryption, thus the data may be easily decoded with free tools available on the Internet. This, in turn, allows to intercept passwords and get unauthorized access to system.

Solution

Set the **snc/enable** parameter to **1** to enable encryption, thus mitigating the risk of unauthorized access. Besides, *the SNC User's Guide* [50] recommendations may be useful that are located at the SAP Help Portal.

- ***[EASAI-NA-27] The SNC encryption to protect RFC connections between systems***

Description

The SAP systems may connect to the other SAP systems, or non-SAP systems using two basic methods:
— with the **Internet Communication Framework (ICF)** that allows to use the HTTP, HTTPS or SMTP, or
— the **Remote Function Call (RFC)** which may be called directly in the system.
The RFC is the proprietary SAP interface for integration between SAP systems and non-SAP system software. The RFC calls a function to execute at a remote system. Other integration technologies, such as web-services, are more often optional in RFC. Currently, there is a whole range of various RFCs, each of them with different properties and for specific purposes.
To ensure security of RFC connections, a wide range of controls may be employed, but this section covers encryption only.

Threat

The RFC-functions called via RFC protocol may transmit confidential data (e.g., passwords or payment card numbers). When using the RFC without encryption, there is a risk of reading this data as plain text. No SNC encryption for RFC connections and no SSL encryption for HTTP connections between the ABAP-based systems enable an adversary to get access to sensitive data by intercepting it with a spoofing attack.

Solution

It is recommended analyse a list of the RFC connections between the ABAP-based systems, for which utilization of the SSL or SNC is required. For security purposes, the connections with the ABAP-based systems must be prevented, where the data is transmitted without the SSL or SNC.

With **SM59** transaction to control RFC and its SNC settings, you may define the following SNC information:
— SNC mode for connection (active or inactive);
— quality of protection (QoP);
— SNC partner name.
Other essential SNC settings (SNC AS name, external library location, maximum and default QoP), as mentioned above, are defined in the application server instance profile (these are profile parameters at the AS ABAP).
To enable the SNC for the RFC adapter and the SAP system, it is necessary to install the certificate on the server. Then, in the RFC screen (the SM59 transaction), for the required RFC connection select the Change option and go to the Security & Logon tab, then switch to Edit --> SNC Options on this tab. In the appeared dialog window "SNC extension: Details" make the following changes:
1) Enter the quality of protection in the QOP field.
2) Enter the SNC communication partner name in the Partners field (if the start of external server program is defined at the application server or at the front end workstation, the SNC partner name will be received automatically from the existing safe route, with no need to specify it).
3) Save the SNC settings.
4) Return to the initial screen and enable SNC.
For the same cases, where the SSL is needed, it is recommended to perform the following actions:
1) execute the **SM59** transaction;
2) select connection for which SSL is required;
3) in the Logon/Security tab, set the SSL option to Activate;
4) save changes.

8. Insecure trusted connections

Various solutions may be used to create intersystem business processes. You may choose weak or intensive interaction depending on the requirements. The so-called trusted relationships between the SAP systems, which are an example of such interaction, allow to minimize the authentication requirements while establishing a remote session. If the calling SAP system accepts the called system as trusted, the password won't be required.
The biggest benefits of such interaction is that, firstly, passwords are not transmitted to the network and, secondly, a simple registration is available beyond the system boundaries. With this function in place, you may create a virtual SAP system which consists of various SAP systems that are called remotely.
Trusted relationships are not mutual, in other words, they are applicable in one direction only. To establish mutual trusted relationships between two systems it is necessary to specify each of them as a trusted one for the associated partner system. It is not surprising that these trusted relationships may include additional security risks.

Further steps

In addition to mechanisms of an application server, servers may often be connected with a number of other mechanisms. SAP solutions, e.g. may be installed on Windows servers which are a part of a single

domain and run with privileges of a common account. In this case, getting access to one server almost always means that to all other servers, no matter how well they are protected at the application level.
Also, it is possible when links or trusted relationships are implemented via DBMS. The DBMS often store references to other databases with pre-defined authentication data thus making other DBMS accessible. Further, the scope of such mechanisms includes any other possible methods to penetrate neighbour system employed in penetration tests, i.e., an attempt to enter the neighbour system with the same or similar passwords both at OS, DBMS and application levels, as well as all kinds of search for passwords in plain text in the file system; update, integration, backup scripts, etc. All this should be checked to eliminate any risk of penetration with one weak link to all systems.

- ***[EASAI-NA-28] RFC connections that store user authentication data***

Description

Many connections between two SAP systems, or a SAP system and an external system (where applications may call ABAP functions at the SAP system, and the SAP systems may call external applications) are based on the *Remote Function Call* **(RFC).** To fully integrate a SAP system in the existed system infrastructure, the provided RFC connections should be identified as RFC destinations. Their incorrect use may lead to risks of compromising the system to which the destinations were created.
There are three categories for the secure ABAP function and RFC logical destination management:
1. Destinations with technical configuration of connections and without stored account credentials and trusted system relationships. They require user authentication for every session, though being highly secure, it's not very convenient, as can't be used automatically in a background mode,
2. Destinations with the technical configuration of connections and account credential (e.g., client, user and password). This method is considered as insecure, as if an adversary gets access to one system, they may connect other systems without password. This check is aimed at elimination of this category.
3. Destinations with the technical configuration of connections using a trusted system logon (trusted/ trusting RFCs). If configured properly, it is the most secure and convenient option.

Threat

With connection storing authentication credentials, an adversary may exploit the user data stored in RFC destinations for unauthorized access to a currently connected system, retrieve sensitive business data and perform any actions there. It happens since RFC connections are often executed under a privileged user with the **SAP_ALL** profile to facilitate administration or data transport. This configuration vulnerability enables successful attacks for many penetration tests.
Access to development systems has often a much weaker protection than that of production systems. Thus, with any vulnerability up to a default password, an adversary may get access to a development system, where they may start the SM59 transaction, select a RFC connection to production system and click the Connect icon. Since connection data is already entered in the system, an adversary automatically gets access to production system. A total attack often requires to make several steps, but access to other servers is anyway possible.

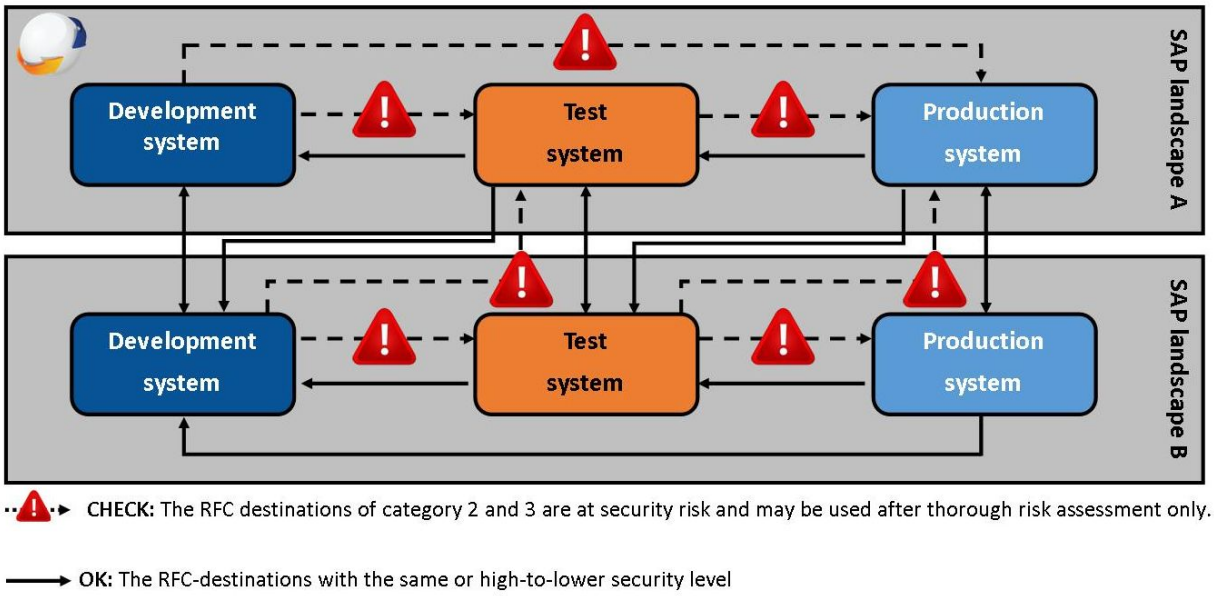
Solution

Check the list of RFC destination storing the authentications credentials, and eliminate such RFC destinations. The stored accounts should be removed wherever is possible, or their privileges should minimized in a remote system . Thus, user must be authenticated for each call (session).
In production systems, users stored in RFC destinations should have only minimum authorizations at the destination point necessary for connection in this business scenario. For this purpose, create a list of RFC destinations storing account data and check that user accounts have minimum authorizations (especially not **SAP_ALL**) assigned at the back-end system. Also, setting the user to **SYSTEM** is important. Use accounts dedicated to scenarios if possible.

- ***[EASAI-NA-29] Trusted systems with low security level***

Description

All RFC destination categories should be used between the systems with the same security level only (which means from one production system to another one), or from a higher security level system to the lower security level systems (for example, from the test system to a development one).
For connections from systems with lower security levels, we don't recommend to store user account data or trusted logons (e.g., from a development system to that of production). Such destinations may store technical configuration of connections only and authenticate users for each session (see the picture).



In addition, higher security level systems should be forbidden to trust lower security level systems at all. Otherwise, the security level of trusting system becomes equal to that of trusted system. The access to trusting systems is controlled with the **S_RFCACL** authorization object.

Threat

An adversary may use configured trusted relationships between systems for unauthorized access to a system and sensitive business data from a lower security level system (being easier to compromise due to weaker security criteria applied in general).

Solution

The following security controls should be implemented to mitigate the risk of an unauthorized access by the RFC destinations:
- All trusted relationships between ABAP-based systems should be checked with **SMT1/SMT2** transactions. Identify trusted high-to-lower security relationships (e.g., a development-to-test or test/development-to-production trusted system relationships) and remove/minimize such system trusts if possible (see SAP Note 128447[51]).
- the RFC authorization checks between systems with the same security level should be enabled with the **auth/rfc_authority_check** profile parameter.
- The authorization object **S_RFCACL** that controls access of trusting systems between those with the same security level should be strictly controlled, and full authorization wildcards (i.e., "*" authorization value) must be forbidden.

9. Logging of security events

One of the most important aspects to ensure the SAP security (and of any other critical system) is security event logging in place. In case of an incident (which is likely to happen because there are a plenty of settings in such systems and it is quite difficult to control all of them), only the security audit configured correctly will allow the company to discover the fact of an attack in time and, perhaps, to arrange a response to it. Besides, the security audit configured correctly allows to prevent attack in the early stages of collecting system data.
The security event logging system is complicated with a lot of different logs for each SAP subsystem, with each of them able to store sensitive information. Unfortunately, few of these logs may be centrally analysed.
This section contains four most critical logs.

Further steps

In total, the SAP system contains about 30 critical and trace logs (for ABAP instance only). After enabling four basic logs described below, implement the fine-tuned settings, e.g., detailed table lists with enabled table logging, details of security event logging in security audit logs, detailed event types in the SAP Gateway log, etc.
Also, their central collection and storage implementation should be accompanied with critical events analysis. Only then, you may add and analyse more detailed optional logs for each service.

- ***[EASAI-NA-30] Logging of security events***

Description

The SAP security audit log is an addition to the system log, but with a slightly different purpose. In contrast to the system log that must be always active, a security audit log may be enabled and disabled if required.
The security audit log is a tool for a detailed overview of all events in a SAP system. The main audit log purpose is to record:
- security-related events in the SAP system neighbourhood (e.g., modifications in primary user accounts);
- information to make system more transparent (e.g., successful and invalid system logon attempts).
- information to reconstruct a chain of events (e.g., successful or failed transaction start).
Filters are used to determine what information should be recorded in the audit log file. In case of event that meets active filter criteria (e.g., start of a transaction), the audit log generates an audit message and writes it to a file. Also, an appropriate notification will be sent to the **CCMS Alert Monitor** (SAP Computing Center Management System Alert Monitor) used to observe centrally the ABAP and Java components, reveal various categories of system and application errors in different interfaces. A detailed information on events is presented in the auditor's report on the audit log vulnerability assessment.
Using filters, you may specify actions needed to be recorded with **SM19** transaction. To review the log, **SM20** transaction is used. **SM18** transaction allows removing old logs.
The audit files are located at individual application servers. You may specify the file location and the maximum file size in the following profile parameters. The basic parameter is
- **rsau/enable,** which enables the audit log on the application server and by default is set to: 0 (inactive audit);

Threat

If the security event registration is not maintained, there is a risk of delayed response (or its absence) to potential external attacks or internal fraud. An opportunity to carry out the Forensic Investigation after the fact of hacking is almost fully excluded, too.

Solution

It is necessary to set the **rsau/enable** parameter to "**1**" (enable) to enable the security event logging. Then, it is necessary to configure filters by specifying exactly what events should be monitored using the SM19 transaction.

- ***[EASAI-NA-31] Logging of HTTP requests***

Description

If the ABAP application server is used for web connections by the ICM service, then it is necessary to configure logging of the HTTP requests to the ABAP application server. The **icm/HTTP/logging_<xx>** parameter is used to manage the HTTP-requests logging in the ICM service (or web dispatcher), if the ICM operates as a server. This parameter defines if HTTP-requests logging is enabled for the ABAP sources. If the ICM acts as a client, you may use the **icm/HTTP/logging_client_<xx>** parameter for the HTTP logging. The **icm/HTTP/*** parameter set is valid for the HTTPS as well.

The parameter syntax looks the following way:
icm/HTTP/logging_<xx>=PREFIX=<URL prefix>, LOGFILE=<log file name> [LOGFORMAT=<format>, FILTER=<filter>, MAXSIZEKB=<size in KBytes>, SWITCHTF=<options>, FILEWRAP=on]
The **LOGFILE** parameter value determines the output file name in the file system. The HTTP-requests logging is not executed if the LOGFILE value is not specified.

Threat

If the security event registration is not maintained, there is a risk of delayed response (or its absence) to potential attacks with the HTTP protocol use. These logs are highly critical, in case the ICM service has the Internet access. Forensic Investigations of an incident related to the Internet attacks is almost impossible with these service logs disabled.

Solution

Specify the OS file name in the **icm/HTTP/logging_<xx>** parameter in the **LOGFILE** value to collect all necessary information on potential attacks. It is essential for a Forensic Investigation.

- ***[EASAI-NA-32] Logging of table changes***

Description

All SAP data are presented in tables. There are two different table categories:
1. Client tables. They contain data used for one client (mandant) only, e.g., the user system logon data in **USR02**.
2. Cross-client or client independent tables. These contain data valid for all the system clients, such as, for example, the **T000** table.
The SAP provides table modification logging option to determine what a user has changed, added or removed in the data from tables and when. There are two technical requirements; with both of them in place, you may be sure that table modifications are logged:
- the general logging should be enabled;
- the technical table parameters should be set to "Record data changes".
The data recorded for these modifications is stored in the **DBTABLOG** table (**DBTABPRT** in lower versions). For them, the **BC_DBLOGS** archiving object may be used.
General logging
The table changes are not logged by default. Activate the associated settings for the selected clients through the **rec/client** system parameter. This parameter may have the following values:
— **OFF** (disabled logging),
— **All** (logging is enabled for all the system clients),
— **<Client number>, (...)** (logging for clients with the numbers filled in here).
This parameter covers only those table modifications that result from direct system changes. The modifications occurred as a result of transport activities (for example, import) do not interact with this parameter ("Logging through transports" is used for this).
Attention (!): the changes are not recorded when copying client.
Table logging

The table logging is controlled by an appropriate value in the technical table configuration (for display, the **SE13** transaction is used). To review all the tables logged, the **DD09L** table is called with the **SE16N** transaction. It works with the tables where:
- the maximum number of characters in the key field is 250;
- the maximum number of character in the data fields is 3500;

Transport logging

To log modifications resulted from transport activities, set up the associated transport parameters. These parameters may be enabled in the *Transport Management System* (**TMS**) with the **STMS** transaction. The desired values for the transport profile (*All, <Client number>*) are set in the **recclient** parameter (see SAP Note 163694 [52]).

Threat

With no direct table access logging, there is a risk of late or no response to potential unauthorized table data modifications, e.g., an adversary may change the bank account value in the *LFBK* table and commit fraud actions by money transfer to another account.

Solution

- You should change the **rec/client** parameter to values corresponding to all production client numbers to collect all required information for a potential Forensic Investigation.
- Automatic logging is not recommended in test systems, as this may lead to a very rapid disk space fill.
- You should log all specific tables with all transaction, system control, setting and other main data, as well as all the data where logging is under question.
- For production system, you should log all clients (*rec/client = ALL*), at least those of production. But if you set the rec/client parameter to ALL you may seriously affect the system performance.
- For more information, see the following notes: 1916, 112388, 84052. [53] [54] [55]

- ***[EASAI-NA-33] Logging of SAP Gateway activities***

Description

Each SAP instance has the **SAP Gateway**. The gateway ensures interaction between work processes and external programs, and also interaction between the work processes from different instances or SAP systems. The gateway allows to execute RFC services at a SAP system.
Higher security requirements are applied to a gateway since it is an application server interface with other systems (other SAP systems, external programs, etc.), one of these requirements is gateway logging activation.
The gateway logging is used to control the gateway activity. You may configure what gateway actions exactly will be recorded in the log file.
It is possible to configure the log maintenance in the **gw/logging** parameter or in the gateway monitor (the **SMGW** transaction). Notice that the gateway monitor is not available if a separate gateway or the Java-only installation are used.

The parameter *gw/logging* contains various indicators that are responsible for logging of certain event types. The S indicator (i.e. Security) in the ACTION field is the most important allowing to record security configuration events and their modifications (e.g., file reloading), with other event types being also important.

Threat

With no security event logging, there is a risk of late or no response to potential attacks on a gateway. The risk of a security breach is considerably increased by this service vulnerabilities known since 2007 and exploits available on the Internet and that enables to get unauthorized access to the service and execute any OS commands.

Solution

- Add **S** value to the **ACTION** field for the **gw/logging** parameter to increase the security level and gain all information required for the potential Forensic Investigation.
- Logging of other security event types is also advisable.

About the company

ERPScan is an award-winning innovative company founded in 2010, honored as the Most innovative security company by Global Excellence Awards as well as Emerging Vendor by CRN, and the leading SAP AG partner in discovering and solving security vulnerabilities. **ERPScan** is engaged in ERP and business application security, particularly SAP, and the development of SAP system security monitoring, compliance, and cybercrime prevention software. Besides, the company renders consulting services for secure configuration, development, and implementation of SAP systems which are used by SAP AG and Fortune 500 companies, and conducts comprehensive assessments and penetration testing of custom solutions.

Our flagship product is **ERPScan** Security Monitoring Suite for SAP: award-winning innovative software and the only solution on the market to assess and monitor 4 tiers of SAP security: vulnerability assessment, source code review, SoD conflicts, and SIEM/forensics. The software is successfully used by the largest companies from industries like oil and gas, nuclear, banking, logistics, and avionics as well as by consulting companies from South Africa to Australia. **ERPScan** is a unique product which enables conducting a complex security assessment and monitoring SAP security afterwards. **ERPScan** is an easily deployable solution which scans basic SAP security configuration in 5 minutes and several clicks. **ERPScan** was designed to work in enterprise systems and continuously monitor changes for multiple SAP systems. These features enable central management of SAP system security with minimal time and effort.

The company's expertise is based on research conducted by the **ERPScan** research subdivision which is engaged in vulnerability research and analysis of critical enterprise applications and gain multiple acknowledgments from biggest software vendors like SAP, Oracle, IBM, VMware, Adobe, HP, Kaspersky, Apache, and Alcatel for finding 350+ vulnerabilities in their solutions. **ERPScan** experts are frequent speakers in 40+ prime international conferences held in USA, Europe, CEMEA, and Asia, such as BlackHat, RSA, HITB, and Defcon. **ERPScan** researchers lead project EAS-SEC, which is focused on enterprise application security. **ERPScan** experts were interviewed by top media resources and specialized infosec sources worldwide such as Reuters, Yahoo news, CIO, PCWorld, DarkReading, Heise, Chinabyte. We have highly qualified experts in staff with experience in many different fields of security, from web applications and mobile/embedded to reverse engineering and ICS/SCADA systems, accumulating their experience to conduct research in SAP system security.

Bibliography

[1] "*The website of company focused on SAP Security solutions. ERPScan)* [Online]. Available: http://erpscan.com

[2] "Association of Certified Fraud Examiners," [Online]. Available: http://www.acfe.com/.

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

[4] "SAP Security: attacking SAP clients," [Online]. Available: http://erpscan.com/publications/sap-security-attacking-sap-clients/.

[5] "CanSecWest conference report by Steve Lord, Mandalorian," [Online]. Available: http://cansecwest.com/slides06/csw06-lord.ppt.

[6] "ERPScan's SAP Pentesting Tool," [Online]. Available: http://erpscan.com/products/erpscan-pentesting-tool/.

[7] "ERPScan WEBXML Checker," [Online]. Available: http://erpscan.com/products/erpscan-webxml-checker/.

[8] "Sapyto – SAP Penetration Testing Framework," [Online]. Available: http://www.cybsec.com/EN/research/sapyto.php.

[9] "EAS-SEC," [Online]. Available: http://eas-sec.org/.

[10] "The Open Web Application Security Project (OWASP)," [Online]. Available: https://www.owasp.org/index.php/Main_Page.

[11] "*SAP security in figures 2011"* [Online]. Available:

http://erpscan.com/wp-content/uploads/2012/06/SAP-Security-in-figures-a-global-survey-2007-2011-final.pdf

[12] "*SAP security in figures 2013"* [Online]. Available: http://www.rsaconference.com/writable/presentations/file_upload/das-t03_final.pdf.

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

[14] "Enterprise Business Application Vulnerability Statistics," [Online]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Vulnerability_Statistics.

[15] "Enterprise Business Application Security Vulnerability Testing Guide," [Online]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Security_Vulnerability_Testing_Guide_v1.

[16] "Enterprise Business Application Security Software," [Online]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Security_Software.

[17] "Enterprise Business Application Security Implementation Assessment Guide," [Online]. Available: https://www.owasp.org/index.php/Enterprise_Business_Application_Security_Implementation_Assessment_Guide.

[18] "Acknowledgments to Security Researchers," [Online]. Available: http://scn.sap.com/docs/DOC-8218.

[19] "SAP Software Update Manager Tool – SPS Update Demo – Part I," [Online]. Available: http://scn.sap.com/docs/DOC-25113.

[20] "SAP Support Portal," [Online]. Available: https://websmp205.sap-ag.de/support.

[21] "How to update SAP Kernel using SUM," [Online]. Available: http://sapbasismania.net/2012/10/how-to-update-sap-kernel-using-SUM.html.

[22] "Password Control in SAP Systems," [Online]. Available: http://www.sapsecurityonline.com/password_sap.htm.

[23] "SAP Note 68048," [Online]. Available: https://service.sap.com/sap/support/notes/68048.

[24] "SAP Note 1414256," [Online]. Available: https://service.sap.com/sap/support/notes/1414256.

[25] "SAP Note 761637," [Online]. Available: https://service.sap.com/sap/support/notes/761637.

[26] "Secure Configuration of SAP NetWeaver Application Server Using ABAP," [Online]. Available:

http://scn.sap.com/docs/DOC-17149.

[27] "Security, Audit and Control Features SAP ERP, ISACA," [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Audit-and-Control-Features-SAP-ERP-3rd-Edition.aspx.

[28] "TCP/IP Ports Used by SAP Applications," [Online]. Available: http://scn.sap.com/docs/DOC-17124.

[29] "SAP Start Service," [Online]. Available: http://help.sap.com/saphelp_nw73ehp1/helpdata/en/b3/903925c34a45e28a2861b59c3c5623/content.htm.

[30] "SAP Note 1600846," [Online]. Available: https://service.sap.com/sap/support/notes/1600846.

[31] "SAP Note 927637," [Online]. Available: https://service.sap.com/sap/support/notes/927637.

[32] "SAP Note 1439348," [Online]. Available: https://service.sap.com/sap/support/notes/1439348.

[33] "Architectural Overview of SAP Host Agent," [Online]. Available: http://help.sap.com/saphelp_nw70ehp3/helpdata/en/a9/02f459814347619d80560e65a7f7d5/content.htm?frameset=/en/21/98c443122744efae67c0352033691d/frameset.htm.

[34] "SAP Note 1341333," [Online]. Available: https://service.sap.com/sap/support/notes/1341333.

[35] "SAP Note 1816536," [Online]. Available: https://service.sap.com/sap/support/notes/1816536.

[36] "SAP NetWeaver," [Online]. Available: http://help.sap.com/netweaver.

[37] "SAP Note 1480644," [Online]. Available: https://service.sap.com/sap/support/notes/1480644.

[38] "SAP Note 1105897," [Online]. Available: https://service.sap.com/sap/support/notes/1105897.

[39] "SAP Note 1473017," [Online]. Available: https://service.sap.com/sap/support/notes/1473017.

[40] "SAP Note 1069911," [Online]. Available: https://service.sap.com/sap/support/notes/1069911.

[41] "SAP Note 1425765," [Online]. Available: https://service.sap.com/sap/support/notes/1425765.

[42] "SAP Note 1408081," [Online]. Available: https://service.sap.com/sap/support/notes/1408081.

[43] "SAP Note 1434117," [Online]. Available: https://service.sap.com/sap/support/notes/1434117.

[44] "SAP Note 614971," [Online]. Available: https://service.sap.com/sap/support/notes/614971.

[45] "SAP Note 1525125," [Online]. Available: https://service.sap.com/sap/support/notes/1525125.

[46] "ITAF, Information Technology Assurance Framework," [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/ITAF2ndEd.pdf.

[47] "Data Protection Guidelines for SAP ERP 6.0," [Online]. Available: http://www.dsag.de/fileadmin/media/Leitfaeden/110818_Leitfaden_Datenschutz_Englisch_final.pdf.

[48] "How to protect ABAP application servers against BEAST-attacks) [Online]. Available: http://sapland.ru/blogs/polyakov/?post=8238.

[49] "SSL Configuration in SAP ABAP AS and JAVA AS – Step-by-step procedure," [Online]. Available: http://scn.sap.com/docs/DOC-26144.

[50] "SNC User's Guide," [Online]. Available: http://help.sap.com/saphelp_nw70ehp1/helpdata/en/23/3a91f8d1724bc6b9e693eb735bcf2f/content.htm?frameset=/en/e6/56f466e99a11d1a5b00000e835363f/frameset.htm.

[51] "SAP Note 128447," [Online]. Available: https://service.sap.com/sap/support/notes/128447.

[52] "SAP Note 163694," [Online]. Available: https://service.sap.com/sap/support/notes/163694.

[53] "SAP Note 1916," [Online]. Available: https://service.sap.com/sap/support/notes/1916.

[54] "SAP Note 112388," [Online]. Available: https://service.sap.com/sap/support/notes/112388.

[55] "SAP Note 84052," [Online]. Available: https://service.sap.com/sap/support/notes/84052.

Additional information sources

1. *CORE Labs Discovery of Six Vulnerabilities within SAP Netweaver*, http://blog.coresecurity.com/2012/05/09/core-labs-discovery-of-six-vulnerabilities-within-sap-netweaver/#sthash.E97e8DUy.dpuf
2. *The ERP Security Challenge*, http://cio.com/article/216940/The_ERP_Security_Challenge
3. *Common Vulnerabilities and Exposures*, http://cve.mitre.org
4. *BlackHat EU 2011 Wiegenstein The ABAP Underverse WP*, http://ebookbrowsee.net/blackhat-eu-2011-wiegenstein-the-abap-underverse-wp-pdf-d147369592
5. *SAP Netweaver XRFC — Stack Overflow*, http://erpscan.com/advisories/dsecrg-10-005-sap-netweaver-xrfc-%E2%80%94-stack-overflow/
6. *SAP NetWeaver SLD – Information Disclosure*, http://erpscan.com/advisories/dsecrg-11-023-sap-netweaver-sld-information-disclosure/
7. *NetWeaver BCB – Missing Authorization/Information disclosure*, http://erpscan.com/advisories/dsecrg-11-027-netweaver-bcb-%E2%80%93-missing-authorization-information-disclosure/
8. *SAP NetWeaver SOAP RFC – Denial of Service / Integer overflow*, http://erpscan.com/advisories/dsecrg-11-029-sap-netweaver-soap-rfc-%E2%80%93-denial-of-service-integer-overflow/
9. *SAP NetWeaver – Authentication bypass (Verb Tampering)*, http://erpscan.com/advisories/dsecrg-11-041-sap-netweaver-authentication-bypass-verb-tampering/
10. *SAP Application Server Security essentials: default passwords*, http://erpscan.com/press-center/blog/sap-application-server-security-essentials-default-passwords/
11. *SAP Infrastructure security internals: Google and Shodan hacking for SAP*, http://erpscan.com/press-center/blog/sap-infrastructure-security-internals-google-and-shodan-hacking-for-sap/
12. *Architecture and program vulnerabilities in SAP's J2EE engine*, http://erpscan.com/wp-content/uploads/2011/08/A-crushing-blow-at-the-heart-SAP-J2EE-engine_whitepaper.pdf
13. *Top 10 most interesting SAP vulnerabilities and attacks*, http://erpscan.com/wp-content/uploads/2012/06/Top-10-most-interesting-vulnerabilities-and-attacks-in-SAP-2012-InfoSecurity-Kuwait.pdf

14. *SAP NetWeaver TH_GREP module - Code injection vulnerability (NEW)*, http://erpscan.ru/advisories/dsecrg-11-039-sap-netweaver-th_grep-module-code-injection-vulnerability-new/

15. *Exploit Database by Offensive Security*, http://exploit-db.com

16. *Invoker Servlet*, http://help.sap.com/saphelp_nw70ehp2/helpdata/en/bb/f2b9d88ba4e8459e5a69cb513597ec/frameset.htm

17. *SAP Management Console Information Disclosure*, http://onapsis.com/resources/get.php?resid=adv_onapsis-2011-002

18. *TCP/IP Ports Used by SAP Applications*, http://scn.sap.com/docs/DOC-17124

19. *Vulnerability Database*, http://securityfocus.com

20. *Systems Applications Proxy Pwnage*, http://sensepost.com/cms/resources/labs/tools/poc/sapcap/44con_2011_release.pdf

21. *SAP (in)security: Scrubbing SAP clean with SOAP*, http://slideshare.net/ChrisJohnRiley/sap-insecurity-scrubbing-sap-clean-with-soap

22. *SAP: Session (Fixation) Attacks and Protections (in Web Applications)*, http://taddong.com/docs/BlackHat_EU_2011_Siles_SAP_Session-Slides.pdf

23. *SQL Injection with ABAP*, http://virtualforge.com/tl_files/Theme/Presentations/HITB2011.pdf

24. *PROTECTING JAVA AND ABAP BASED SAP APPLICATIONS AGAINST COMMON ATTACKS,* http://virtualforge.com/tl_files/Theme/whitepapers/201106_SAP_Security_Recommendations_Protecting_JAVA_ABAP.pdf

Our contacts

E-mail: info@erpscan.com

PR: press@erpscan.com

Web: www.erpscan.com