Top 10 most interesting SAP vulnerabilities and attacks
Alexander Polyakov CTO ERPSan

12 October 2012 at HackTivity
ERPScan
Security Scanner for SAP

Me

Business application security expert

HACKTIVITY
What is SAP?

Shut up
And
Pay
• The most popular business application
• SAP has 183000 customers
• 74% of Forbes 500
Agenda

• Intro
• SAP security history
• SAP on the Internet
• Most popular SAP issues
• Top 10 latest interesting attacks
• DEMOs
• Conclusion
3 areas of SAP Security

- Business logic security (SOD)
  - Prevents attacks or mistakes made by insiders
  - Solution: GRC

- ABAP Code security
  - Prevents attacks or mistakes made by developers
  - Solution: Code audit

- Application platform security
  - Prevents unauthorized access both within the corporate network and from remote attackers
  - Solution?
Talks about SAP security

Most popular:
- BlackHat
- HITB
- Troopers
- RSA
- Source
- DeepSec
- etc.
By June, 2012, more than 2300 notes
SAP vulnerabilities by type

1 - Directory Traversal
2 - XSS/Unauthorised modification of stored content
3 - Missing Auth check
4 - Information Disclosure
5 - Unauthorized usage of application functionality
6 - Hard-coded credentials
7 - Code injection vulnerability
8 - Verb tampering
9 - Remote Code Execution
10 - Denial of service
11 - BOF
12 - SQL Inj

Stats from:
- 1Q 2012
- 1Q 2010
- 4Q 2009
Top problems by OWASP-EAS

- EASAI-1 Lack of patch management
- EASAI-2 Default Passwords for application access
- EASAI-3 SOD conflicts
- EASAI-4 Unnecessary Enabled Application features
- EASAI-5 Open Remote management interfaces
- EASAI-6 lack of password lockout/complexity checks
- EASAI-7 Insecure options
- EASAI-8 Unencrypted communications
- EASAI-9 Insecure trust relations
- EASAI-10 Guest access
Top problems by BIZEC

- BIZEC TEC-01: Vulnerable Software in Use
- BIZEC TEC-02: Standard Users with Default Passwords
- BIZEC TEC-03: Unsecured SAP Gateway
- BIZEC TEC-04: Unsecured SAP/Oracle authentication
- BIZEC TEC-05: Insecure RFC interfaces
- BIZEC TEC-06: Insufficient Security Audit Logging
- BIZEC TEC-07: Unsecured SAP Message Server
- BIZEC TEC-08: Dangerous SAP Web Applications
- BIZEC TEC-09: Unprotected Access to Administration Services
- BIZEC TEC-10: Insecure Network Environment
- BIZEC TEC-11: Unencrypted Communications
Business Risks

Espionage
- Stealing financial information
- Stealing corporate secrets
- Stealing suppliers and customers list
- Stealing HR data

Sabotage
- Denial of service
- Modification of financial reports
- Access to technology network (SCADA) by trust relations

Fraud
- False transactions
- Modification of master data
- e.t.c.
We have collected data about SAP systems in the WEB
Have various stats by countries, applications, versions
Information from Google, Shodan, Nmap scan
Published in “SAP Security in figures: a global survey 2007-2011”
Updating results at sapscan.com
2 SAP web services can be found in internet (In Hungary)
> 5000 non-web SAP services exposed in the world

> >50 in Hungary

Including Dispatcher, Message server, SapHostcontrol, etc
SAP in the Internet (other services)

% of companies that expose different services

- SAP Dispatcher
- SAP MMC
- SAP Message Server
- SAP HostControl
- SAP ITS Agate
- SAP Message Server httpd

HUNGARY

WORLD
Top 10 vulnerabilities 2011-2012

1. Authentication Bypass via Verb tampering
2. Authentication Bypass via the Invoker servlet
3. Buffer overflow in ABAP Kernel
4. Code execution via TH_GREP
5. MMC read SESSIONID
6. Remote portscan
7. Encryption in SAPGUI
8. BAPI XSS/SMBRELAY
9. XML Blowup DOS
10. GUI Scripting DOS
• SAP users can run scripts which automate their user functions
• A script has the same rights in SAP as the user who launched it
• Security message which is shown to user can be turned off in the registry
• Almost any user can use SAP Messages (SM02 transaction)
• It is possible to run DOS attack on any user using a simple script
Script can be uploaded using:
- SAPGUI ActiveX vulnerability
- Teensy USB flash
- Any other method of client exploitation

Other attacks like changing banking accounts in LFBK also possible
10 – GUI-scripting: Business risks

Sabotage – High

Espionage – No

Fraud – No

Ease of exploitation – Medium
10 – GUI-scripting: Prevention

- SAP GUI Scripting Security Guide
- Don’t activate SAP GUI Scripting if you do not need it
  sapgui/user_scripting = FALSE (default)
  - Scripting with read only capabilities use the parameter
    - sapgui/user_scripting = TRUE
    - sapgui/user_scripting_set_readonly = TRUE
- Block registry modification on workstations
WEBRFC interface can be used to run RFC functions
By default any user can have access
Can execute at least RFC_PING
SAP NetWeaver is vulnerable to malformed XML packets
It is possible to run DOS attack on server using simple script
It is possible to run over the Internet!
9 – XML Blowup DOS: Business risks

Sabotage – Critical

Espionage – No

Fraud – No

Ease of exploitation – Medium
9 – XML Blowup DOS: Prevention

- Disable WEBRFC
- Prevent unauthorized access to WEBRFC using S_ICF
- Install SAP notes 1543318 and 1469549 and 139410032
• SAP BAPI transaction fails to properly sanitize input

• Possible to inject JavaScript code or link to a fake SMB server

• SAP GUI clients use Windows so their credentials will be transferred to attackers host.
8 – BAPI script injection/hash stealing
8 – BAPI script injection: Business risks

- Espionage – High
- Sabotage – High
- Fraud – High

Ease of exploitation – Low
8 – BAPI script injection: Prevention

- Install SAP notes 1569550
• SAP FrontEnd can save encrypted passwords in shortcuts
• Shortcuts stored in .sap file
• This password uses byte-XOR algorithm with “secret” key
• Key has the same value for every installation of SAP GUI
• Any password can be decrypted in less than second
7 – SAP GUI bad encryption: Demo

```
$.
```
7 – SAP GUI bad encryption: Business risks

- Espionage – High
- Sabotage – Medium
- Fraud – High
- Ease of exploitation – Medium
Disable password storage in GUI
6 – Remote port scan/SSRF: Description

- It is possible to scan internal network from the Internet
- Authentication is not required
- SAP NetWeaver J2EE engine is vulnerable

/ipcpricing/ui/BufferOverview.jsp?
server=172.16.0.13
& port=31337
& password=
& dispatcher=
& targetClient=
& view=
6 – Remote port scan/SSRF: Demo

**IP Error**

An error has occurred in the IPC.

`ConnectionException: Connection timed out: connect`

This error is fatal. Please restart your session or contact the support.

**Host is not alive**

**Port closed**

**SAP port**

**HTTP port**

**IP Error**

An error has occurred in the IPC.

`ConnectionException: Connection refused: connect`

This error is fatal. Please restart your session or contact the support.
6 – Remote port scan/SSRF: Business risks

- Sabotage – Low
- Espionage – Medium
- Fraud – No
- Ease of exploitation – High
• Disable unnecessary applications
• Install SAP notes:
  1548548, 1545883, 1503856, 948851, 1545883
5 – MMC JSESSIONID stealing: Description

- Remote management of SAP Platform
- By default, many commands go without auth
- Exploits implemented in Metasploit (by ChrisJohnRiley)
- Most of the bugs are information disclosure
- It is possible to find information about JSESSIONID
- Only if trace is ON

1) Original bug by ChrisJohnRiley
2) JSESSIONID by Alexey Sintsov and Alexey Tyurin (ERPScan)

Can be authenticated as an existing user remotely
5 – MMC JSESSIONID stealing: Business risks

Espionage – Critical

Fraud – High

Sabotage – Medium

Ease of exploitation – Medium
Don’t use TRACE_LEVEL = 3 on production systems or delete traces

RCE vulnerability in RFC module TH_GREP

- Found by Joris van de Vis
- SAP was not properly patched (1433101)
- We have discovered that the patch can be bypassed in Windows

Original bug by Joris van de Vis (erp-sec)
Bypass by Alexey Tyurin (ERPScan)
elseif opsys = 'Windows NT'.

concatenate '/c:"" string "" filename into grep_params in character mode.

else. /*if linux*/
    /* 185 */ replace all occurrences of "" in local_string with """"""""
    /* 186 */ concatenate "" local_string "" filename into grep_params
    /* 187*/ in character mode.
    /* 188*/ endif.

/* 188*/
4 – RCE in TH_GREP: Demo #1
4 ways to execute vulnerable program:

• Using transaction "Se37"
• Using transaction “SM51” (thanks to Felix Granados)
• Using remote RFC call "TH_GREP"
• Using SOAP RFC call "TH_GREP" via web
4 – RCE in TH_GREP: Business risks

- Espionage – High
- Sabotage – Medium
- Fraud – High

Ease of exploitation – medium
• Install SAP notes 1580017, 1433101
• Prevent access to critical transactions and RFC functions
• Check the ABAP code of your Z-transactions for similar vulnerabilities
• Presented by Andreas Wiegenstein at BlackHat EU 2011

• Buffer overflow in SAP kernel function C_SAPGPARAM

• When NAME field is more than 108 chars

• Can be exploited by calling an FM which uses C_SAPGPARAM

• Example of report – RSPO_R_SAPGPARAM
3 – ABAP Kernel BOF: Business risks

- Espionage – Critical
- Sabotage – Critical
- Fraud – Critical

Ease of exploitation – Medium
• Install SAP notes:
  - 1493516 – Correcting buffer overflow in ABAP system call
  - 1487330 – Potential remote code execution in SAP Kernel

• Prevent access to critical transactions and RFC functions

• Check the ABAP code of your Z-transactions for critical calls
2 – Invoker Servlet: Description

- Rapidly calls servlets by their class name
- Published by SAP in their security guides
- Possible to call any servlet from the application
- Even if it is not declared in WEB.XML

Can be used for auth bypass
What if we call /servlet/com.sap.admin.Critical.Action
2 – Invoker servlet: Business risks

Espionage – High

Sabotage – High

Fraud – High

Ease of use – Very easy!
2 - Invoker servlet: Prevention

- Update to the latest patch 1467771, 1445998
- “EnableInvokerServletGlobally” must be “false”
- Check all WEB.XML files by ERPScan WEBXML checker
1 – VERB Tampering
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Restrictedaccess</web-resource-name>
    <url-pattern>/admin/*</url-pattern>
    <http-method>GET</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>admin</role-name>
  </auth-constraint>
</security-constraint>

What if we use HEAD instead of GET?
CTC - interface for managing J2EE engine
Can be accessed remotely
Can run user management actions:
  - Add users
  - Add to groups
  - Run OS commands
  - Start/Stop J2EE

Remotely without authentication!
1 – Verb tampering: More details

If patched, can be bypassed by the Invoker servlet!
1 – Verb tampering: Business risks

- Espionage – Critical
- Sabotage – Critical
- Fraud – Critical

Ease of use – Very easy!
1st Place – Verb tampering: Prevention

- Install SAP notes 1503579, 1616259
- Install other SAP notes about Verb Tampering
- Scan applications by ERPScan WEB.XML checker
- Disable the applications that are not necessary
It is possible to be protected from almost all those kinds of issues and we are working hard with SAP to make it secure.

- SAP Guides
- Regular Security assessments
- Monitoring technical security
- ABAP Code review
- Segregation of Duties

It’s all in your hands
Many of the researched things cannot be disclosed now because of our good relationship with SAP Security Response Team, whom I would like to thank for cooperation. However, if you want to see new demos and 0-days, follow us at @erpscan and attend the future presentations:

- 16 October - IT Security Expo (Germany, Nurnberg)
- 30 October - HackerHalted (USA, Miami)
- 2-3 November - HashDays (Switzerland, Lucerne)
- 8-9 November - POC In Korea (Korea, Seul)
- 20 November – ZeroNights (Russia, Moscow)
- 29 November - DeepSEC (Austria, Vienna)
Greetz to our crew who helped: Dmitriy Evdokimov, Alexey Sintsov, Alexey Tyurin, Pavel Kuzmin, Evgeniy Neelov.