Invest in security to secure investments

SAP Security made easy.
How to keep your SAP systems secure

Alexander Polyakov (CTO ERPScan)
About ERPScan

• The only 360-degree SAP Security solution - ERPScan Security Monitoring Suite for SAP
• **Leader** by the number of **acknowledgements from SAP** (150+)
• 60+ presentations **key security conferences worldwide**
• 25 Awards and nominations
• Research team - **20 experts with experience in different areas of security**
• Headquartered in Palo Alto (US) and Amsterdam (EU)
• Working together since 2007

“We would like to thank the world-class security experts of ERPScan for the highly qualified job performed to help us assess the security of our pre-release products”.

Senior Director, Head of Global Security Alliance Management
Product Security, Technology and Innovation Platform
SAP Labs, Palo Alto, USA
Client needs

- How to protect ourselves from fraud and cyber-attacks?
- How to automate security monitoring for big landscapes and get smart reports?
- How to prioritize updates?
- How to comply with regulations?
- How to identify and test most critical vulnerabilities in SAP
- How to address industry-specific solutions’ security?
2007 – Architecture vulnerabilities in RFC protocol
2008 – Attacks via SAPGUI
2009 – SAP backdoors
2010 – Attacks via SAP WEB applications
2010 – Stuxnet for SAP
2011 – Architecture and program vulnerabilities in ABAP
2011 – Vulnerabilities in J2EE engine
2012 – Vulnerabilities in SAP solutions (SolMan, Portal, XI) and Services Dispatcher, Message Server
2012 – Vulnerabilities in Protocols - XML, DIAG
2013 – SAP Forensics and Anti-forensics
2014 – SAP BusinessObjects, SAP HANA and other specific platforms

Research talks
about SAP security in technical conferences

How to prevent?

New threats
• 3000+ Vulnerabilities in all SAP Products
• 2368 Vulnerabilities were found in SAP NetWeaver ABAP based systems
• 1050 Vulnerabilities were found in basic components which are the same for every system
• About 350 Vulnerabilities were found in ECC modules.

By November 2014 – 3200+ notes
Public vulnerabilities

Security expert warns of way to attack SAP systems

(Reuters) - A software security expert warned that flaws in the design of business management software from SAP AG can allow hackers to easily break into Proof of Concept Code.

The following python script is the main PoC that can be used to reproduce all vulnerabilities described below:

```python
connection.connect(('hostname, port'))
# Send initialization packet
print ("[*] Connected, sending login request"
init = 'ALLYMESSAGE\x00' # eyecatcher
init += '\x04' # version
init += '\x00' # errorno
init += client_string # toname
init += '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
init += '\x01\x08' # flag /iflag (MS_LOGIN_2)
init += client_string # fromname
init += '\x00\x00' # padd
send_packet(connection, init)

# Receive response
print ("[*] Receiving login reply"
(length, data) = receive(connection, init)
```

SAP Netweaver Dispatcher Multiple Vulnerabilities
Is A Tsunami Of SAP Attacks Coming?

Ericka Chickowski

New banking Trojan modification points to greater trend of attackers targeting ERP and business critical applications.

New incidents have been discovered in recent months, with some involving malware variants that exploit vulnerabilities in SAP-powered systems.

The malware, known as Troj/SAP-Banks Trojan, was found to infect a number of SAP-based systems, including those used by large enterprises.

Security

Nvidia takes customer site offline after SAP bug found

Jeremy Kirk

Jan 8, 2014 6:40 PM

Graphics chipmaker Nvidia took a customer service website offline Wednesday following a report of a vulnerability in its SAP-powered backend.

The affected website, https://nvcare.nvidia.com, uses SAP's NetWeaver, which is a critical for the company's operations.

Incidents

New malware variant suggests cybercriminals targeting SAP users

Lucian Constantin, IDG News Service

Nov 1, 2013 3:20 AM

A new variant of a Trojan program that targets online banking accounts also contains code to search for infected computers and then download additional malware, according to security researchers.

Campaign4Change

Breaking down barriers to change
Why should we care

- Espionage
  - Theft of financial information
  - Corporate trade secret theft
  - Theft of supplier and customer lists
  - Stealing HR data Employee Data Theft
- Sabotage
  - Denial of service
  - Tampering with financial reports
  - Access to technology network (SCADA) by trust relations
- Fraud
  - False transactions
  - Modification of master data
• Manipulate data about quantity of material resources (S)
• Blocking of materials for posting (S)
• Changing the goods’ price (F,S)
• Changing tolerance limits for operations (F,S)
• Money stealing (F)
• Changing credit limits
• Modification of price by changing conditions (F,S)
• Stealing credit card data (E)
• Modification of financial reports (S)

*Risks: (S-sabotage, F – fraud, E- espionage)*
• SAP is owned and managed by business
• Businesses rarely care about security (only SOD )
• CISO’s sometimes don’t even know about SAP
• CISO’s care about infrastructure security
• But if breach will happen it will be their responsibility

Our mission is to close this gap.
• **Complexity**
  Complexity kills security. Many different vulnerabilities in all levels, from network to application

• **Customization**
  Cannot be installed out of the box. They have many (up to 50%) custom codes and business logic

• **Risky**
  Rarely updated because administrators are scared they can be broken during updates; also, it is downtime

• **Unknown**
  SAP is Mostly available inside the company (closed world). Research and Pentest community is not familiar with it
Myth 1: SAP Systems applications are only available internally what means no threat from the Internet

Myth 2: SAP security is a vendor’s problem

Myth 3: SAP application internals are very specific and are not known for hackers

Myth 4: SAP security is all about SOD
3 areas of SAP Security

Business logic security (SOD)
Prevents attacks or mistakes made by insiders

Custom Code security
Prevents attacks or mistakes made by developers

Application platform security
Prevents unauthorized access both within corporate network and from remote attackers
• Current security solutions like VA, SIEM, AST embody very little SAP coverage
• Solutions focused on SAP Security are more effective but only cover any one of listed fields each and they are not “CISO-oriented”
• We see solution
  – Platform for everybody
  – Coverage of all aspects
  – Complimentary to SAP offerings or extend them
The only award-winning solution in the market to assess 3 tiers of SAP Security
Architecture

Presentation

Control

Connectors

- SAP Admin
- CISO
- Risk Manager
- ABAP Developer
- Pentester

- SIEM
- IT GRC

- SIEM
- ITSM
- Ticketing

- ERP
- CRM
- SRM
- HANA
- BOBJ
- Mobile

Vulnerability Management module
Source code security module
SOD module
In details

Presentation level

Security Metrics
Statistics (Trends)
Comparison
Export
Reports

Control functions

Project management
Risk Management
Template management
Notification Management
Landscape management
Task Management

Vulnerability Management

- Pentest
- Whitebox
- Patches
- Exploitation
- Compliance
- Passwords

- ABAP
- JAVA
- HANA
- Business Objects
- Mobile
- Database

Source Code Security

- Backdoors
- Vulnerabilities

- ABAP
- JAVA

Segregation of Duties

- Role optimization
- Critical privileges
- SoD

- By System
- By Module
- By Industry

Connectors

- SOAP
- SAP Router
- HTTP
- JAVA
- ABAP
- HANA
- BOBJ
- SUP
- Oracle DB

erpscan.com
ERPSan – Invest In Security To Secure Investments
How to automate security monitoring for big landscapes?

- Case: CISO of large Oil company
- Need: To automate monitoring and get high-level reports for 100+ systems.
- Solution:
  - Configure weekly scans covering most critical assets
  - Export results to IBM Qradar for correlation and a consolidated summary of relevant indicators at a glance.
  - Configure PPTX presentations email with the ‘high-level overview’.
How to prioritize updates?

• Case: BASIS team of every organization
• Need: To minimize downtime of systems during updates and prioritize updates.
• Solution:
  – Scan for missing SAP security notes
  – Scan for remotely exploitable vulnerabilities (blackbox)
  – System correlate this data, an you can filter results by 10+ different criteria's to understand risk

<table>
<thead>
<tr>
<th>St</th>
<th>SAP note</th>
<th>Application</th>
<th>Release</th>
<th>SAP</th>
<th>C</th>
<th>Critical</th>
<th>Probability</th>
<th>Exploitability</th>
<th>Threat</th>
<th>Vulnerability type</th>
<th>E.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1553907</td>
<td>BC-DWB-TOO-F</td>
<td>10-05-2011</td>
<td>Hot</td>
<td>8.7</td>
<td>High</td>
<td>High</td>
<td>Public advisor</td>
<td>Internal</td>
<td>Missing authorization check</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1567862</td>
<td>BW-BEX-OT</td>
<td>10-05-2011</td>
<td>Hot</td>
<td>8.2</td>
<td>High</td>
<td>High</td>
<td>Public advisor</td>
<td>Internal</td>
<td>Missing authorization check</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1741239</td>
<td>BC-WD-ABA-RE</td>
<td>14-05-2013</td>
<td>Correct</td>
<td>7.5</td>
<td>Critical</td>
<td>Medium</td>
<td>Details not pub</td>
<td>Internal</td>
<td>Directory traversal</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1604055</td>
<td>FIN-FSCM-TRM</td>
<td>13-09-2011</td>
<td>Hot</td>
<td>7.5</td>
<td>High</td>
<td>Medium</td>
<td>Public advisor</td>
<td>Internal</td>
<td>Hardcoded Credentials</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1563062</td>
<td>FIN-FSCM-TRM</td>
<td>13-09-2011</td>
<td>Hot</td>
<td>7.5</td>
<td>High</td>
<td>Medium</td>
<td>Public advisor</td>
<td>Internal</td>
<td>Hardcoded Credentials</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1667805</td>
<td>CO-OM</td>
<td>14-02-2012</td>
<td>Hot</td>
<td>7.5</td>
<td>Critical</td>
<td>High</td>
<td>Public advisor</td>
<td>Internal</td>
<td>Missing authorization check</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1607529</td>
<td>BC-CCM-MON</td>
<td>14-02-2012</td>
<td>Correct</td>
<td>7.5</td>
<td>Critical</td>
<td>High</td>
<td>Public advisor</td>
<td>Internal</td>
<td>Missing authorization check</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1607850</td>
<td>BW-WHM-DBA-</td>
<td>13-03-2012</td>
<td>Hot</td>
<td>7.5</td>
<td>Medium</td>
<td>Critical</td>
<td>Public advisor</td>
<td>External</td>
<td>Information disclosure</td>
<td></td>
</tr>
</tbody>
</table>
Need: To comply with industry regulations and chose step by step approach for better technical compliance

Solution:
- Scan to address PCI DSS, SOX or NERC CIP regulations
- Step by step technical compliance approach EAS-SEC, SAP Guidelines, ISACA, DSAG
- Add Industry-related checks and guidelines (Oil and Gas, Banking, Retail), make your own template

We have included templates for all of them
How to identify and test most critical vulnerabilities in SAP?

- Case: Security consulting company
- Need: To provide SAP Security assessment and penetration testing services with minimum time
- Solution:
  - Vulnerability management module
  - Blackbox pentesting, exploits, business-focused payloads
• Advanced user management
• Multiple scans’ comparison and efficiency analysis
• Customizable Templates and Landscapes
• Ability to assign tasks to users
• Ability to manage risks
• Largest Built-in knowledge base
• Only 360-degree approach can help in maximizing security
• Specific checks for Industry modules and solutions
• Fast release cycles to address client needs
• Combination of modules gives you more visibility 1+1+1=4
Each SAP landscape is unique and we pay close attention to the requirements of our customers and prospects. ERPScan development team constantly addresses these specific needs and is actively involved in product advancement. If you wish to know whether our scanner addresses a particular aspect, or simply have a feature wish list, please e-mail us or give us a call. We will be glad to consider your suggestions for the next releases or monthly updates.