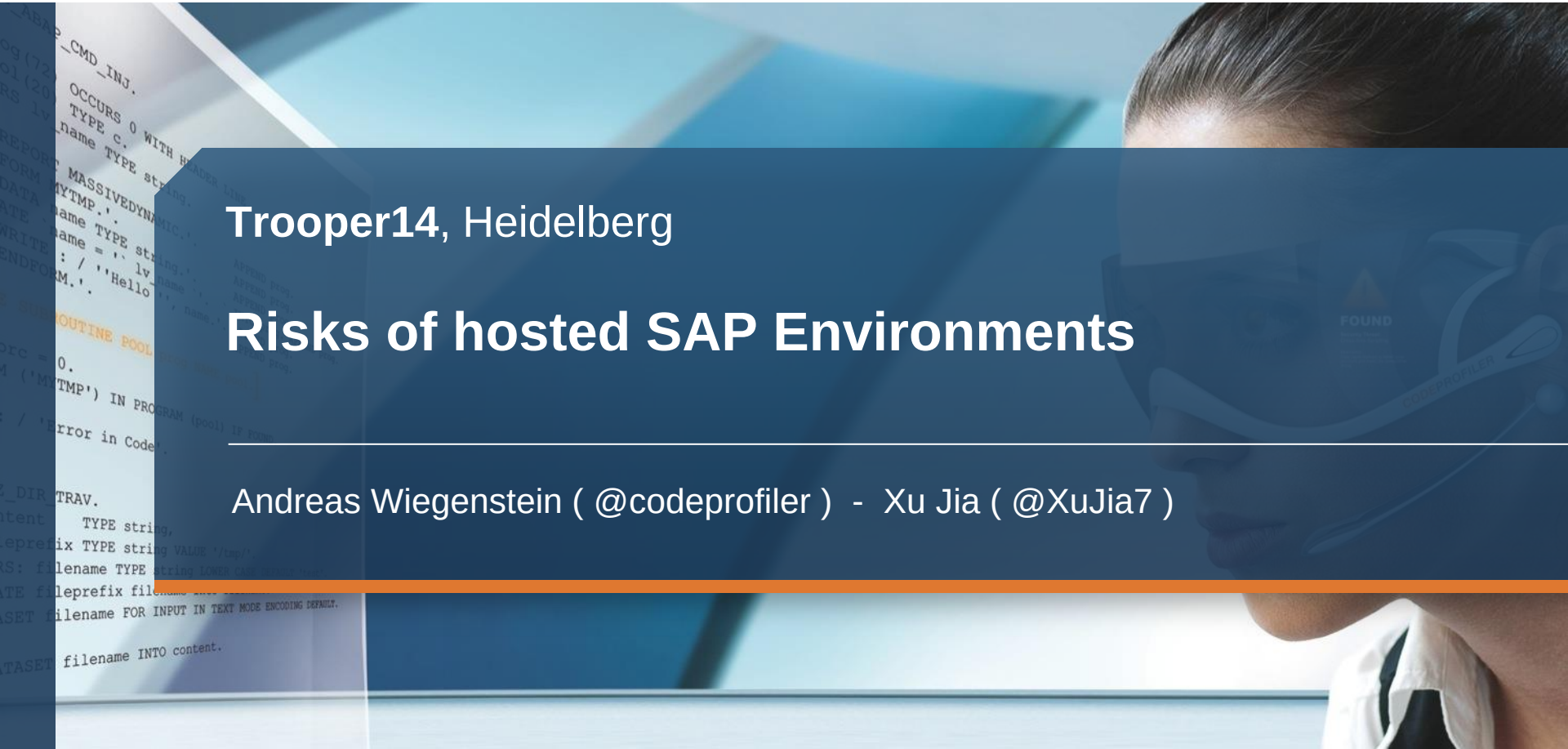
VIRTUALFORGE
run your business safer



Trooper14, Heidelberg

Risks of hosted SAP Environments

Andreas Wiegenstein (@codeprofiler) - Xu Jia (@XuJia7)

Disclaimer

SAP, R/3, ABAP, SAP GUI, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only.

The authors assume no responsibility for errors or omissions in this document. The authors do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

The authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document. Especially not in hosted environments.

#SAP
#Security
#Research

Andreas Wiegenstein

- CTO at Virtual Forge
- SAP Security Researcher, active since 2003
  - Received Credits from SAP for **66** reported 0-day Vulnerabilities
- Speaker at international Conferences
  - **SAP TechEd** (US & Europe), **BlackHat** (Europe), **Hack in the Box** (Europe)
  - **Troopers** (Europe), **IT Defense** (Europe), **RSA** (US)

Xu Jia

- Security Analyst at Virtual Forge
- SAP Security Researcher, active since 2006
  - Received Credits from SAP for **28** reported 0-day Vulnerabilities
- Speaker at international Conferences
  - **Troopers** (2013), **Sicherheit und Prüfung von SAP Systemen** (2012)

Who is SAP?

Why protect SAP Systems?

- More than 248,500 companies run SAP
- SAP customers…
  - → Transport > 1.1 billion flight passengers per year
  - → Produce > 65% of all TV's
  - → Produce > 77,000 cars every day
  - → Produce > 52% of all movies
- And…
  - → 72% of the world-wide beer production depends on companies that run SAP !!!

Source: http://www.posters.at/the-simpsons--homer-bier_a34273.html

#Statistics

"There are three kinds of lies: lies, damned lies, and statistics."

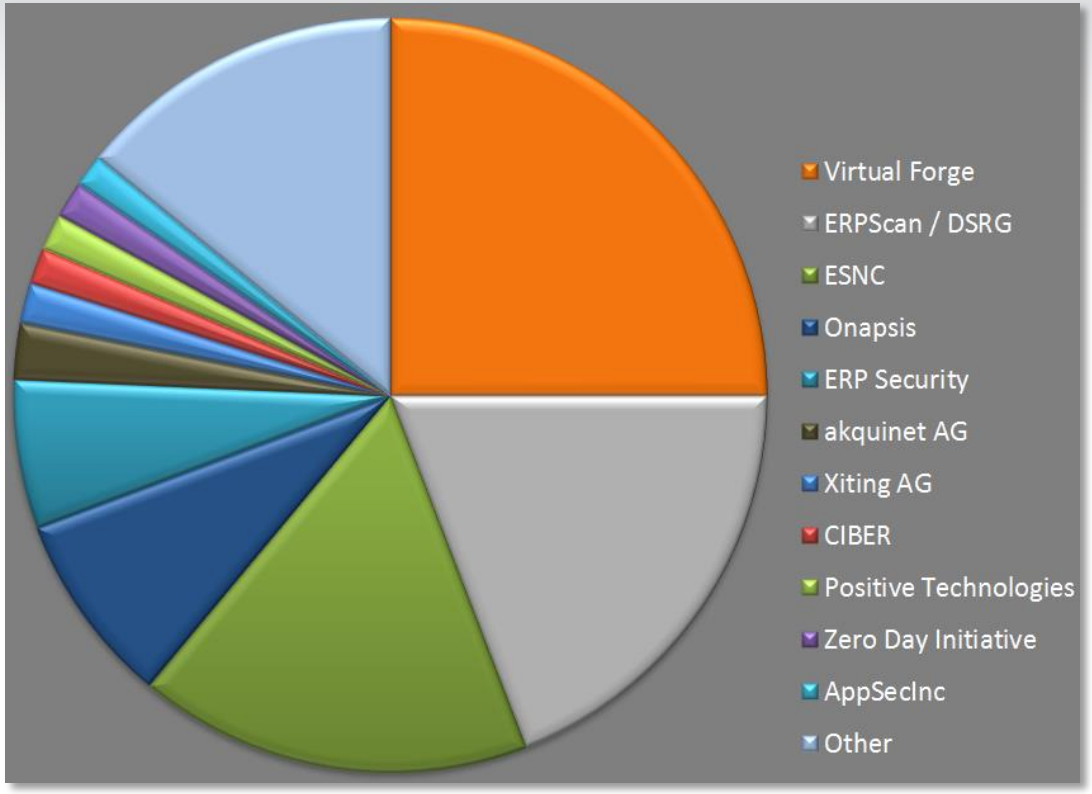
Benjamin Disraeli

“Statistics are mendacious truths.”

Lionel Strachey

“Don’t trust statistics you didn’t falsify yourself.”

Unknown



. . . and now we present

SAP credits* for security advisories

(Since 2010)

5 Companies hold 75%

* Based the number of credits per individual researcher involved in an advisory

** Considering only such advisories that were researched at Starbucks on a Friday afternoon in Heidelberg ;-)

On SAP Security Notes

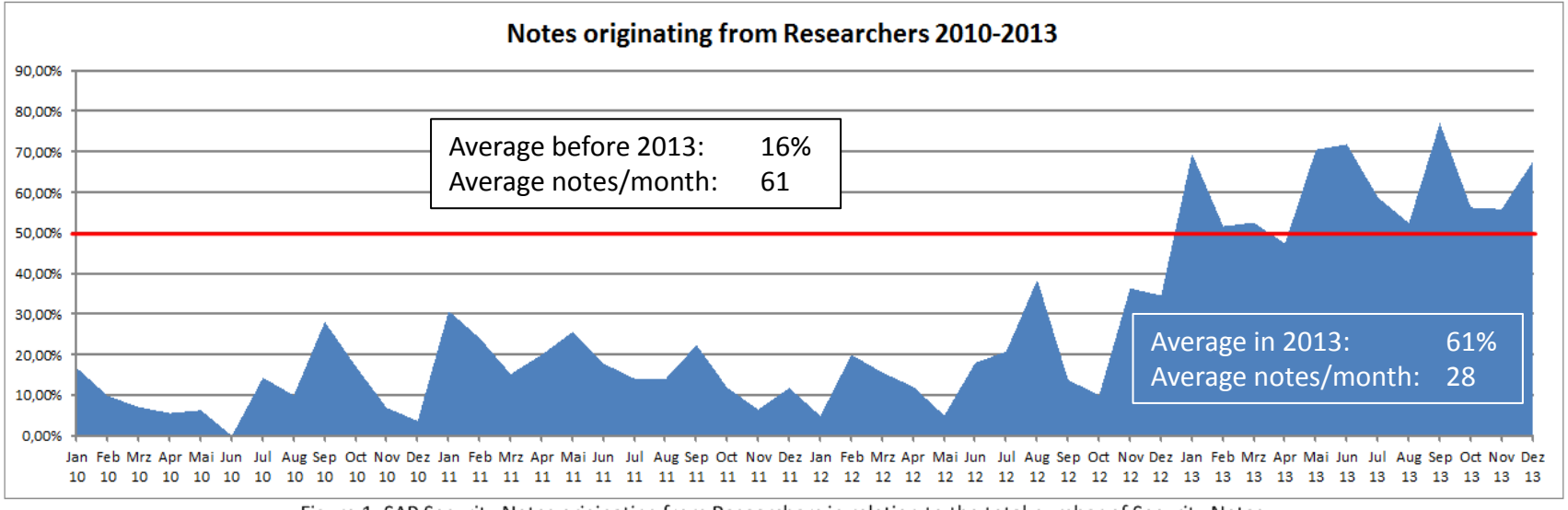


Figure 1: SAP Security Notes originating from Researchers in relation to the total number of Security Notes

Source: https://www.virtualforge.com/de/blog/post/security-research-2013-en.html

Agenda

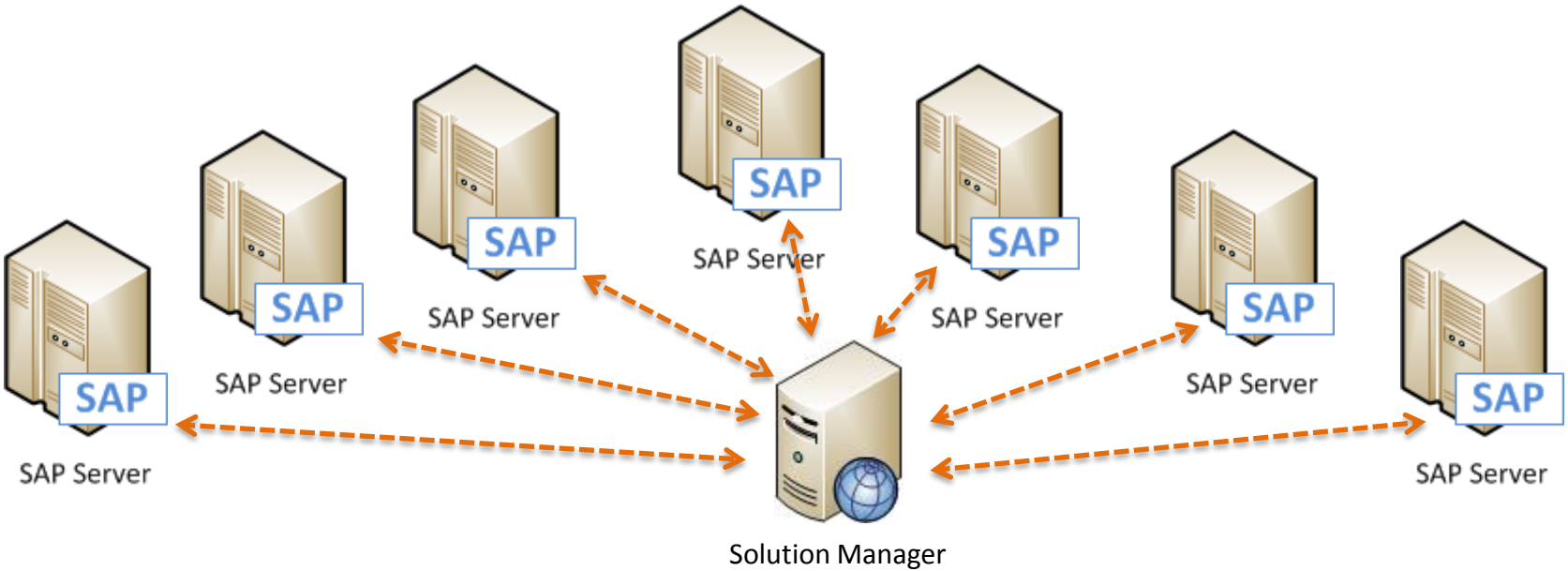
- Motivation
- Hosted SAP Application Variant A : Multi-System
- Hosted SAP Application Variant B : Single-System
- Demo

Motivation

Security Incident

Hosted SAP Application Variant A:

Multi-System



SAP Solution Manager

DEMO

Risks in Multi-System Hosting

SAP Solution Manager (SolMan)

- SolMan has a very high attack surface
- If SAP Solution Manager falls, all connected systems fall
- Many SolMan applications are Web-based
- A critical SAP 0day in SolMan can result in access to all data of all hosted companies

Risks in Multi-System Hosting – SolMan on the Internet

Some URL Patterns of SAP Solution Manager

/sap/bc/webdynpro/sap/ags_workcenter

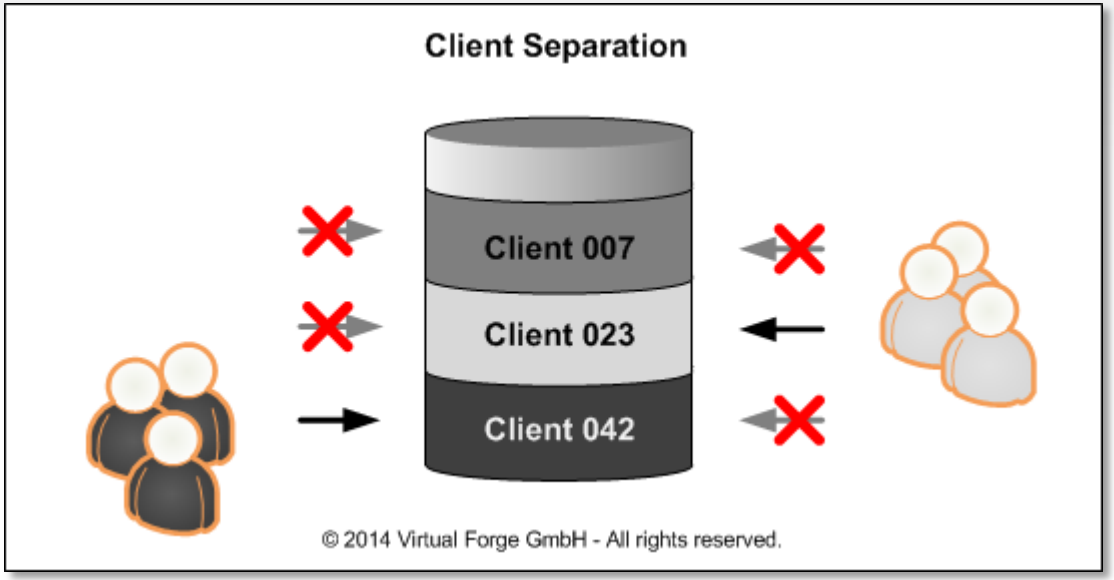
/sap/bc/bsp/sap/ags_rbe_report

/sap/bc/webdynpro/sap/ags_dswp_infra_wc

/sap/bc/webdynpro/sap/ags_work_gui_default_set

Hosted SAP Application Variant B:

Single-System



SAP Open SQL is by design implicitly protecting client-specific data.

Risks in Single-System Hosting – Bypassing Client Protection

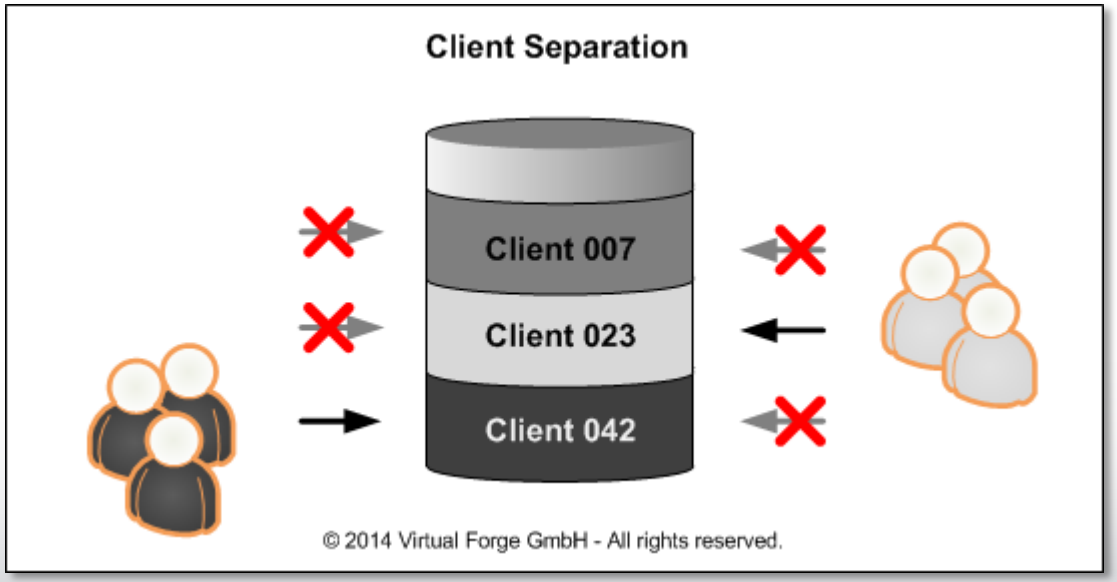
Bypassing OSQL client protection in ABAP programs

- Explicit bypass using CLIENT SPECIFIED
- Implicit bypass using EXECSQL
- Implicit bypass using ADBC

The following Risks exist in Single-System Hosting

- Any custom ABAP Code can access all data of all hosted companies
- Any SAP 0day that allows cross-client access can result in access to all data of all hosted companies
  - -Any ABAP Command Injection Vulnerability
  - -Any Native SQL Injection Vulnerability
  - -Any generic Cross-Client Vulnerability

DEM0day


Client Separation
Client 007
Client 023
Client 042
© 2014 Virtual Forge GmbH - All rights reserved.

Statistics on Cross-Client Access

- Custom code performs on average* 76 cross-client accesses per (in-house) installation

  * Survey of 159 SAP Customers (statistics, again)

- 2000+ occurrences of CLIENT SPECIFIED in SAP Standard

CVSS Guide Version 2.0

http://www.first.org

2.1.4. Confidentiality Impact (C)

Partial (P) There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database.

Complete (C) There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.)

SAP Note (Patch) related to cross-client read Access

1718145	VF Advisory SAP-BACK-13 (generic read Access)
Sent to SAP:	13.02.2012
Patched on:	14.05.2013
Patch time:	451 days
CVSS Rating:	3.5
CVSS Vector:	AV:N/AC:M/AU:S/C:P/I:N/A:N

CVSS Guide Version 2.0

http://www.first.org

2.1.5. Integrity Impact (I)

Partial (P)	Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope.
Complete (C)	There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

CVSS Guide Version 2.0

http://www.first.org

2.1.6 Availability Impact (A)

Partial (P)	There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.
Complete (C)	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

SAP Note (Patch) related to cross-client write Access

1718145	VF Advisory SAP-BACK-12 (generic write Access)
Sent to SAP:	13.02.2012
Patched on:	08.04.2013
Patch time:	415 days
CVSS Rating:	6.0
CVSS Vector:	AV:N/AC:M/AU:S/C:P/I:P/A:P

Summary

(No statistics this time)

Secure Hosting Checklist for SAP Customers

- Does your Hoster install new SAP security notes every month?
- How does your Hoster deal with custom Code Security?
- How does your Hoster mitigate risks related to Solution Manager?
- Are there penetration tests / security audits performed (by SAP security experts) on a regular basis?

SAP Security Blog

This Talk as PDF

Thank you for your attention.

Questions Now or later ?

@codeprofiler @XuJia7

#ThingsWeFoundWhenPentestingSAP