Preventing vulnerabilities in HANA-based deployments

Disclaimer

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

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

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

Agenda

- Introduction
- SAP HANA Architecture and Attack surface
- Cyber-Attacks in HANA platforms
  - TrexNet Attacks
  - Buffer Overflows
  - Remote Passwords retrieval
- Securing SAP HANA
- Conclusions

Introduction

Onapsis overview

Transforming how organizations protect the applications that manage their business-critical processes and information.

- **Founded:** 2009
- **Locations:** Buenos Aires, AR | Boston, MA | Berlin, DE | Lyon, FR
- **Technology**: Onapsis Security Platform (Enterprise Solution)
- **Research:** 300+ SAP and Oracle security advisories and presentations published

Who are we?

Juan Perez-Etchegoyen (JP)
Nahuel Sanchez

- Background on Penetration Testing and vulnerabilities research
- Reported vulnerabilities in diverse SAP and Oracle components
- Authors/Contributors on diverse posts and publications
- Speakers and Trainers at Information Security Conferences
- *http://www.onapsis.com*

A Business-Critical Infrastructure

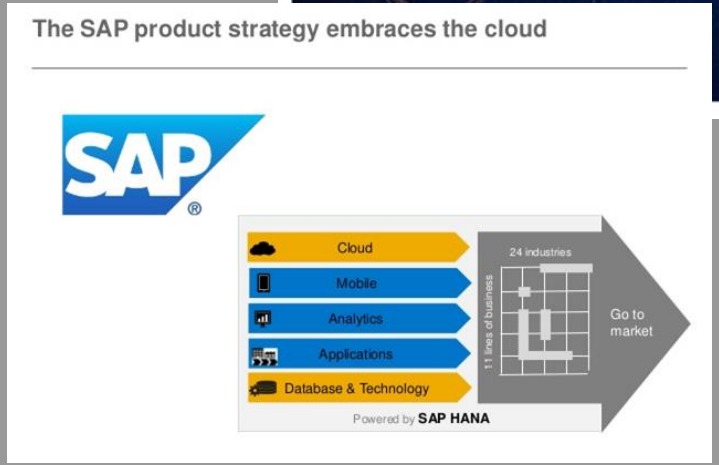
HANA systems store and process the most critical business information in the Organization. If the SAP/HANA platform is breached, an intruder would be able to perform different attacks such as:

- **ESPIONAGE:** Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
- **SABOTAGE:** Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.
- **FRAUD:** Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

An Infrastructure critical for the business

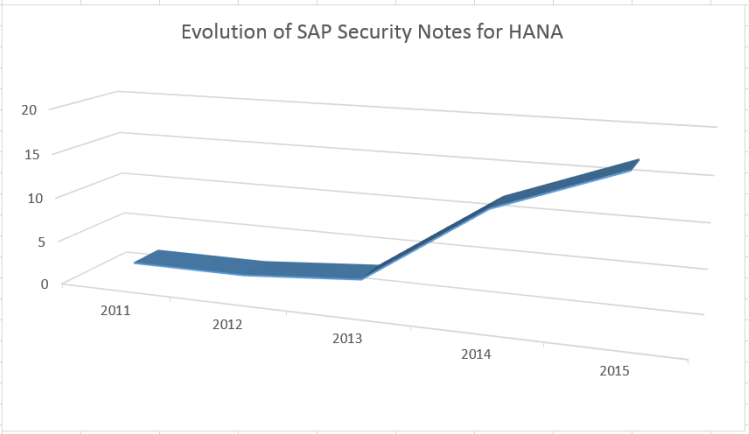
SAP Strategy is shaped around products that run on top of SAP HANA

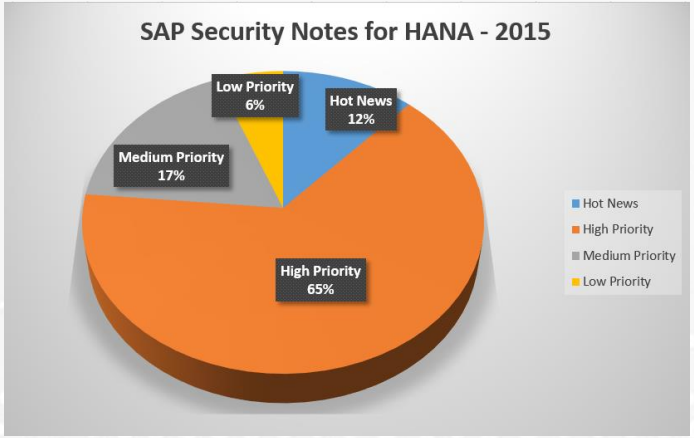
- **PRIVATE CLOUD**
- **PUBLIC CLOUD**
- **S/4HANA**
- **Apps powered by HANA**



Evolution of vulnerabilities in HANA

SAP Security Notes in HANA (2011-2015)





A Dangerous Status-Quo

Key Findings:

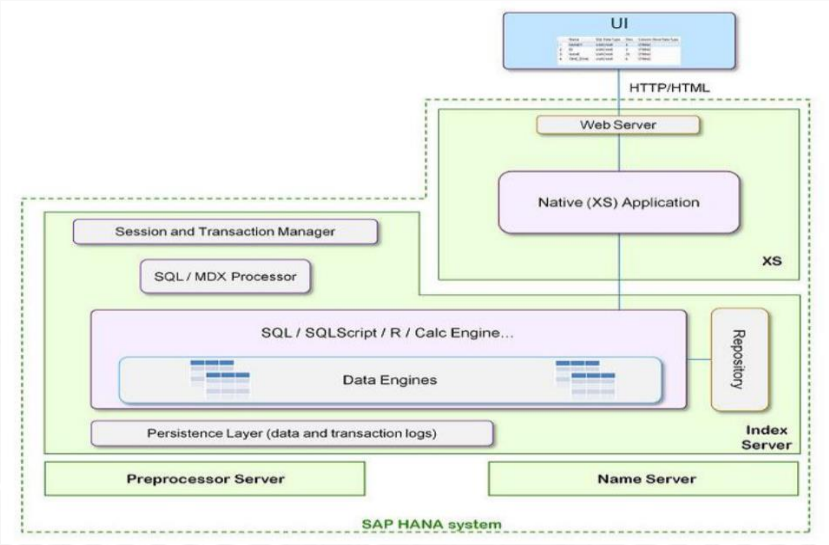
- 75% said their senior leadership understands the importance and criticality of SAP to the bottom line, but only 21% said their leaders are aware of SAP cybersecurity risks.
- 60% said the impact of information theft, modification of data and disruption of business processes on their company's SAP would be catastrophic or very serious.
- 65% said their SAP system was breached at least once in the last 24 months.

Architecture and Attack Surface

SAP HANA ARCHITECTURE

SAP HANA COMPONENTS

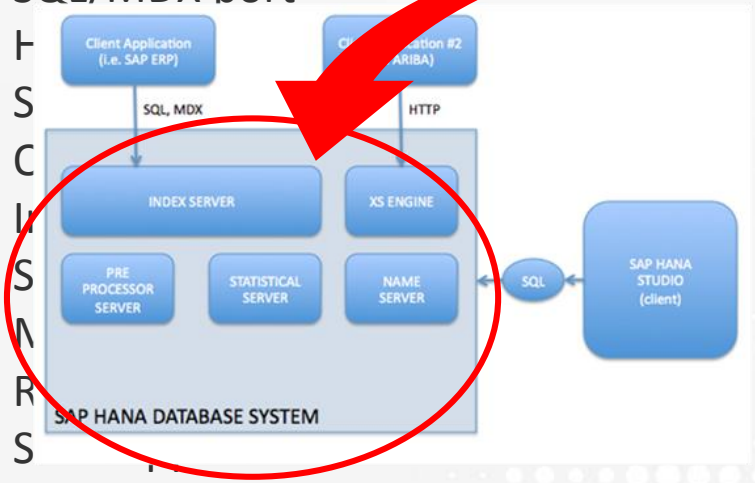
In-memory database
Supports cloud implementations
Integrates with calculation engines
Diverse set of deployment options
Integrated HTTP Server
Used mainly for Business Applications

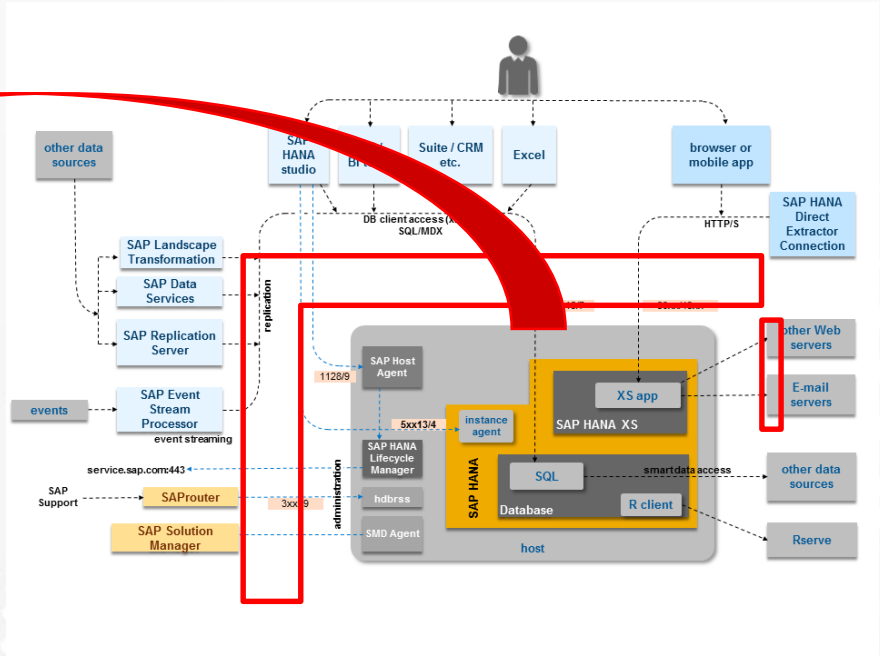


SAP HANA ARCHITECTURE

SAP HANA ENTRY POINTS

SQL/MDX port



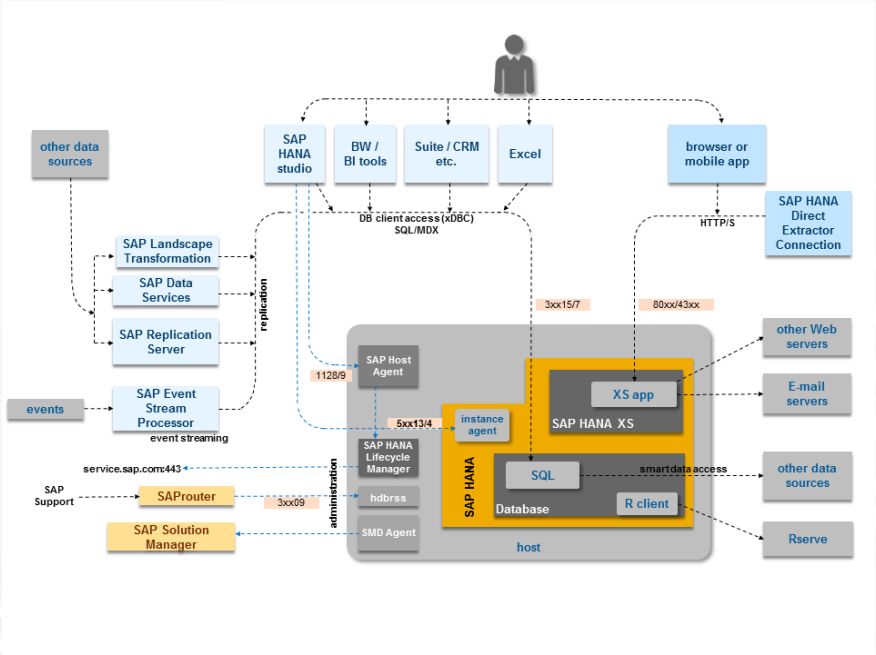


http://help.sap.com/saphelp_hanaplatform/helpdata/en/37/d2573cb24e4d75a23e8577fb4f73b7/content.htm
http://en.community.dell.com/techcenter/b/techcenter/archive/2012/09/28/sap-hana-core-architecture

SAP HANA ARCHITECTURE

SAP HANA PROTOCOLS

Authentication
Authorization
Access Control
Encryption
Mitm Attacks?
DoS Attacks?

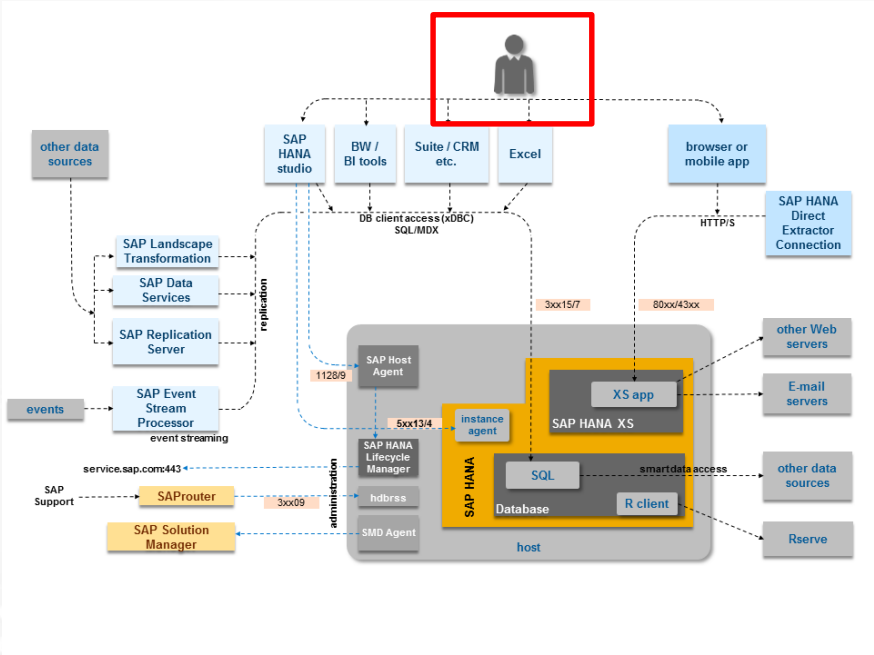


http://help.sap.com/saphelp_hanaplatform/helpdata/en/37/d2573cb24e4d75a23e8577fb4f73b7/content.htm

SAP HANA ARCHITECTURE

SAP HANA WEAKEST LINK

- Database users
- Web Apps users
- HANA Administrators
- Interface users
- Authorizations (System, Application, Object, Analytic, Package, Other users)



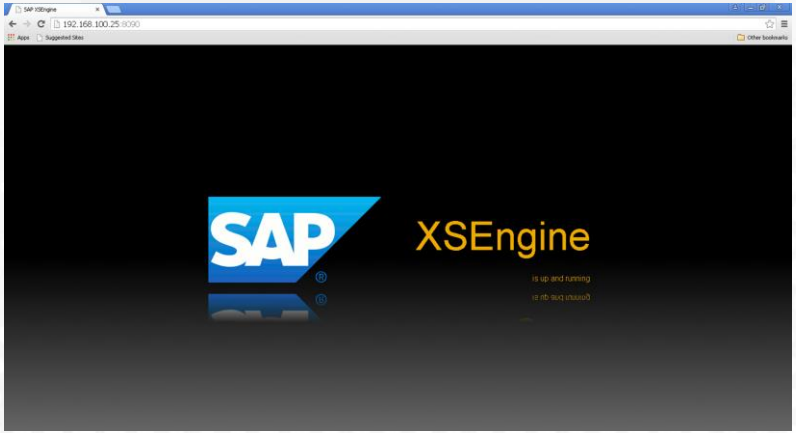
http://help.sap.com/saphelp_hanaplatform/helpdata/en/37/d2573cb24e4d75a23e8577fb4f73b7/content.htm

SAP HANA NETWORK DISCOVERY

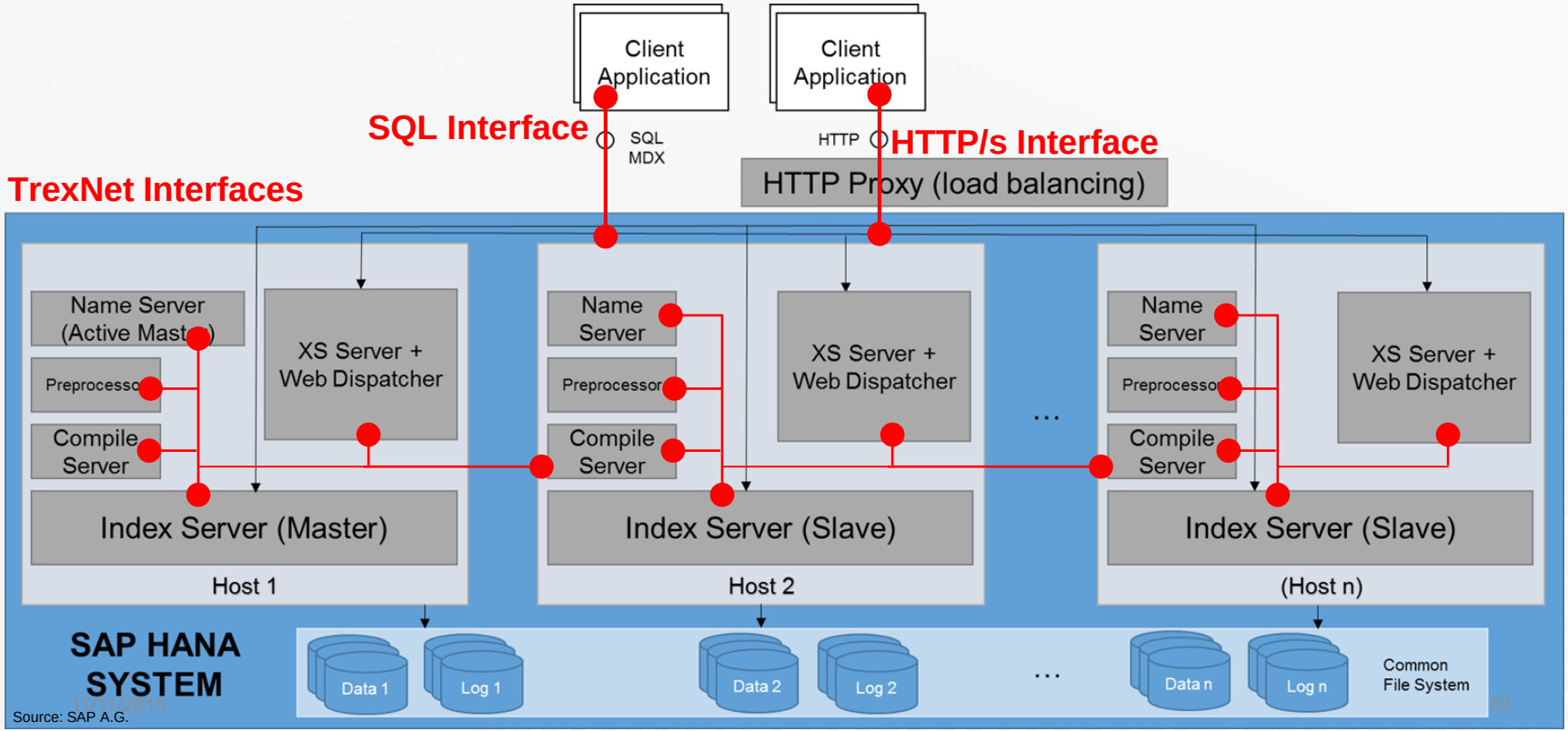
- Network connection
- NMAP
  - Traditional TCP ports pattern (SysNR)
  - New TCP ports pattern
  - HTTP, MDX, MC, HostAgent

- Browser
  - HTTP welcome page
  - Several “public” apps
  - /public/sap/docs/hana/admin/help

```
…
4390/tcp  open  ssl/unknown
8090/tcp  open  unknown
39015/tcp open  tcpwrapped
39017/tcp open  tcpwrapped
59013/tcp open  http      gSOAP httpd 2.7
59014/tcp open  ssl/http  gSOAP httpd 2.7
…
```



SAP HANA Architecture & Entry points



Source: SAP A.G.

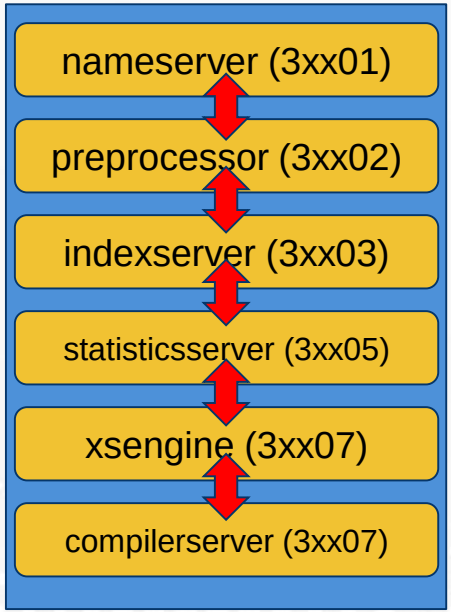
TrexNet Attacks to SAP HANA

(CVE-2015-7828)

onapsis

SAP HANA Architecture & TrexNet

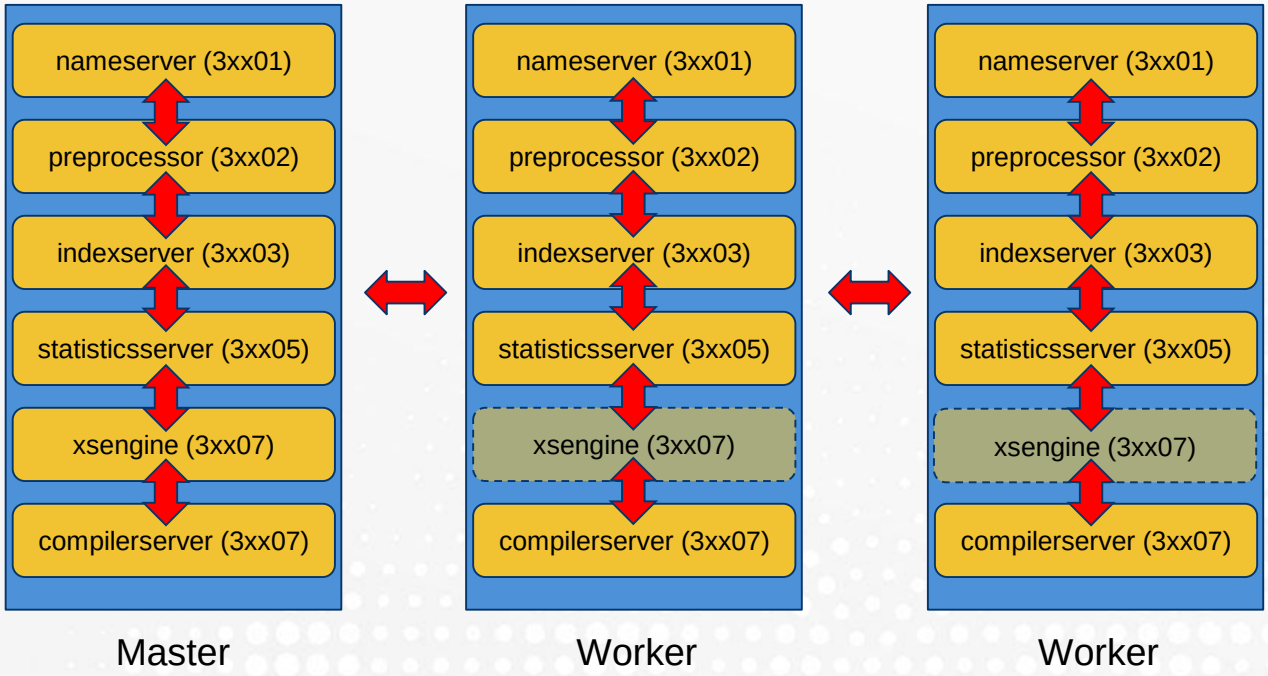
- Single host scenario
- TrexNet Protocol
  - Custom
  - Undocumented
  - Inherited from Trex



SAP HANA Host 1

SAP HANA Architecture & TrexNet contd.

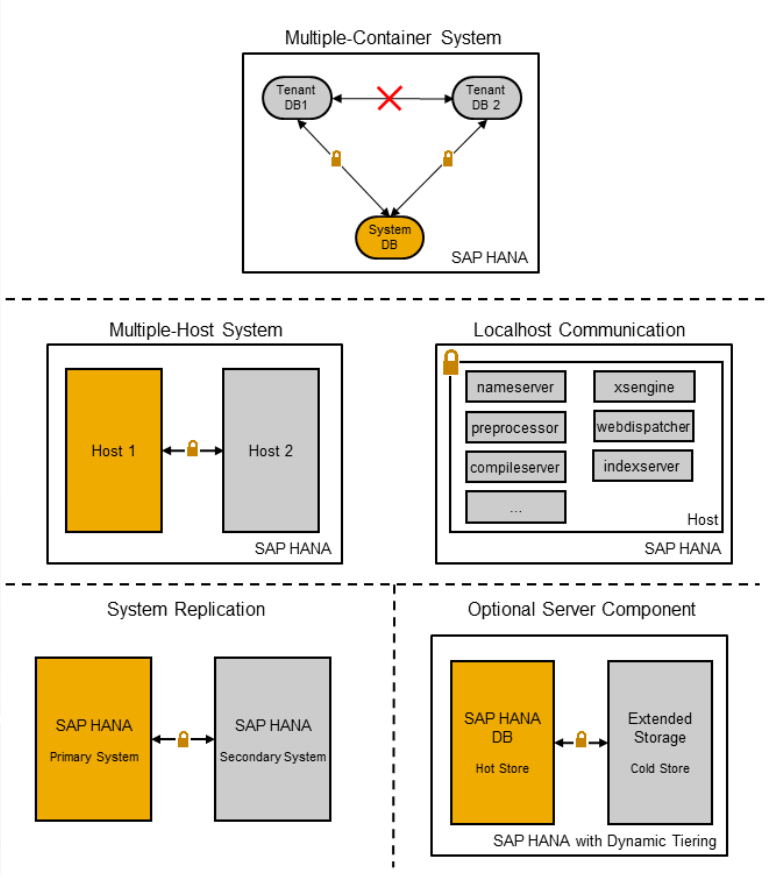
- Distributed scenario
- TrexNet Protocol
  - Mandatory
  - Host comm.
  - Replication, HA
  - Hardening required



TrexNet Security

- Unauthenticated protocol
- listens on localhost **(SPS06)**
- SSL enabled by default for internal communications (SPS10)
- Different configuration options

- **Critical vulnerabilities fixed after Onapsis report**
  - Arbitrary File Read/Write
  - Remote DoS
  - Python code Execution
  - others...



https://help.sap.com/saphelp_hanaplatform/helpdata/en/de/f770d6bb5710149f32a6c5593f5877/content.htm

DEMO #1

Exploitation of TrexNet protocols demo

What happened?

- Remote unauthenticated user (NO USER NEEDED)
- Network access to specific SAP HANA services
- Attacker can trigger specific unauthenticated functionality in HANA
- After a successful execution, sidadm privileges are obtained → equivalent to FULL SYSTEM COMPROMISE

Solution

- Implement a secure configuration (SAP Security Note 2183363).
- Use a dedicated network for the “Internal communications”.
- Enable SSL if not enabled by default, follow SAP HANA Security guide.

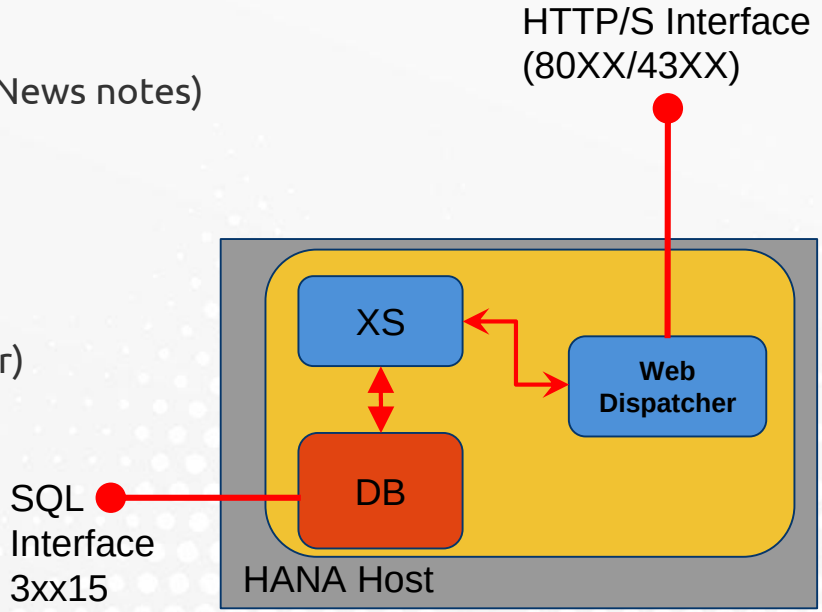
Buffer overflows in SAP HANA

(CVE-2015-7993) and (CVE-2015-7993)

onapsis

Overview

- Discovered by Onapsis
- **Highly critical vulnerabilities** (patched by Hot News notes)
- **Full compromise**
  - Cloud services
  - OS isolation
- Hard to code reliable exploits (more on this later)
- **Remote unauthenticated DoS otherwise**



DEMO #2

Exploitation of buffer overflows in HANA

What happened?

- Remote unauthenticated user (NO USER NEEDED)
- Access to HANA HTTP interface (potentially internet/cloud)
- Triggers a buffer overflow in the HANA system
- After a successful exploitation, potentially sidadm could be obtained → FULL SYSTEM COMPROMISE

Solution

- **Implement SAP Security Notes 2197397 and 2197428.**
- If possible, restrict access to HTTP and/or SQL interfaces only to trusted networks.

HTTP Login Remote Code Execution (CVE-2015-7993) Analysis

- Pre auth. Heap overflow in process hdbindexserver
- Triggered by a long username or password
- Vulnerable function “HandleAuthRequest”
  - **memcpy use!**
  - Plenty of space to write payload
  - Objects in the heap are overwritten
- Different lengths of the username / Password will overwrite different objects. This leads to different crashes that are hard to control / predict.

HTTP Login Remote Code Execution (CVE-2015-7993) Analysis

- Suse Linux used as underlying OS.
  - **System-wide ASLR enabled by default**
- hdbindexserver process (SPS09)
  - **NX bit enabled**
  - **PIE enabled**
- Information leak vulnerability required!
- Heap massaging

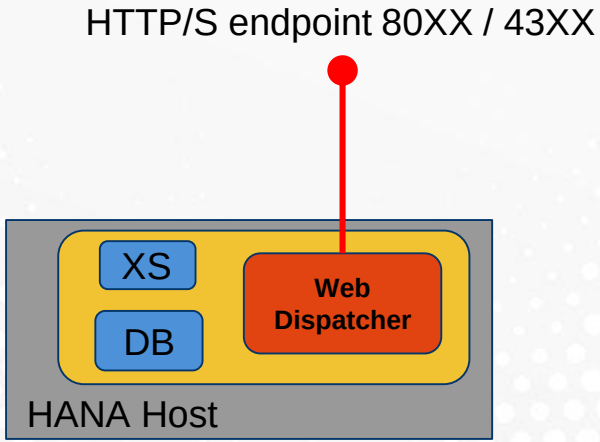
Remote Passwords retrieval in SAP HANA

(CVE-2015-7991)

onapsis

Sensitive information logging & Remote trace disclosure

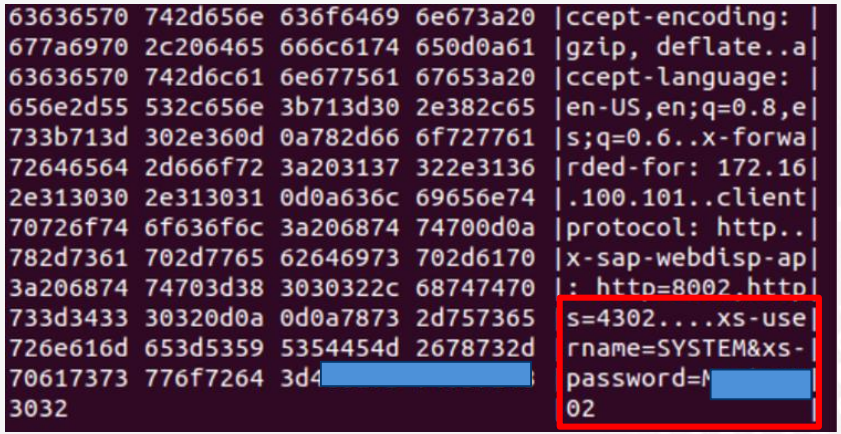
- Components affected: Internal web dispatcher & Standalone web dispatcher
  - Handles HTTP/s requests
  - Web configuration is possible
    - “/sap/wdisp/admin” URL



- Can be configured to log every HTTP request
  - sapwebdisp.pfl / webdispatcher.ini
- Trace level can be configured

Sensitive information logging & Remote trace disclosure

- **if Trace level > 2, Passwords are logged in plaintext! (VULNERABILITY #1)**
- Trace files can be downloaded
  - **Without any prior authentication! (VULNERABILITY #2)**



http://<IP>:<PORT>/sap/hana/xs/wdisp/admin/download?ftype=0

http://<IP>:<PORT>/sap/hana/xs/wdisp/admin/download?ftype=1

DEMO #3

Remote Passwords retrieval demo

What happened?

- Remote unauthenticated user (NO USER NEEDED)
- Access to HANA HTTP interface (potentially internet/cloud)
- Uses the browser to access a specific url
- Downloads HANA traces and parses them looking for passwords
- Once the attacker got access credentials, he connects back to the target system
- Depending on the privileges of the retrieved credentials, the attacker could compromise the HANA system and its information

Solution

- **Implement security notes 2148854, 2011786 and 1990354**
- Restrict network access to reduce attack surface whenever possible

So, How do we protect HANA?

How do we protect our HANA systems?

Develop Secure Applications

Restrict packages exposed via http
Secure authentication methods required web apps
Use restricted user types for HTTP apps.
Enable Cross-Site-Request Forgery (XSRF) Protection
Validate all parameters! (There are protections but only to “help” developers)

Secure HANA communications

Configure SSL for all communications.
Force the use of SSL.
Restrict access at network level.
Secure the certificates and establish a proper key management procedure.

How do we protect our HANA systems?

Secure user access to HANA

Secure the standard SYSTEM user.
Secure <sid>adm user.
Use restricted users if possible.
Use SSO (Single Sign-On) mechanisms.
Implement strong password policies.

Assign minimum required privileges

System privileges
Object privileges
Analytic privileges
Package privileges
Application privileges
User privileges

How do we protect our HANA systems?

Secure the data in HANA

Understand HANA encryption
Use encryption for sensitive data
Establish a proper key management procedure
Change default keys!

Enable Logs and Traces

Enable audit log
Restrict Audit Roles
Secure access to:
Audit Trail DB Table, default_audit_trail_path,
UIS.sap.hana.uis.db::DEFAULT_AUDIT_TBL, Trace and dump files

How do we protect our HANA systems?

Secure the data in HANA

Understand HANA encryption
Use encryption for sensitive data

but specially… Apply the latest patches to secure HANA systems and keep up with the latest SAP Security Notes!

Restrict Audit Roles
Secure access to:
Audit Trail DB Table, default_audit_trail_path,
UIS.sap.hana.uis.db::DEFAULT_AUDIT_TBL, Trace and dump files

Conclusions

- Keep the HANA systems updated with the latest patches should not be optional
- SAP HANA was built with a security focus, however many responsibilities rely on the **users** (administrators, developers, end users…)
- Specialized **resources and software** can help you to securely configure and detect security vulnerabilities on SAP HANA systems.
- Keep up with SAP Documentation:

  Read the SAP HANA Security Guide :
  http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf

  Follow SAP HANA Security Whitepaper which gives an overview of HANA Security as a good starting point: http://www.saphana.com/docs/DOC-3751

  SAP HANA Developer Guide which contains information on secure programming practices: http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf

  A good guide which gives information on how to build standard roles in HANA:
  https://scn.sap.com/docs/DOC-53974

QUESTIONS?
THANKS!

onapsis