


# Layer Seven Security

SAP Security Notes

July 2017



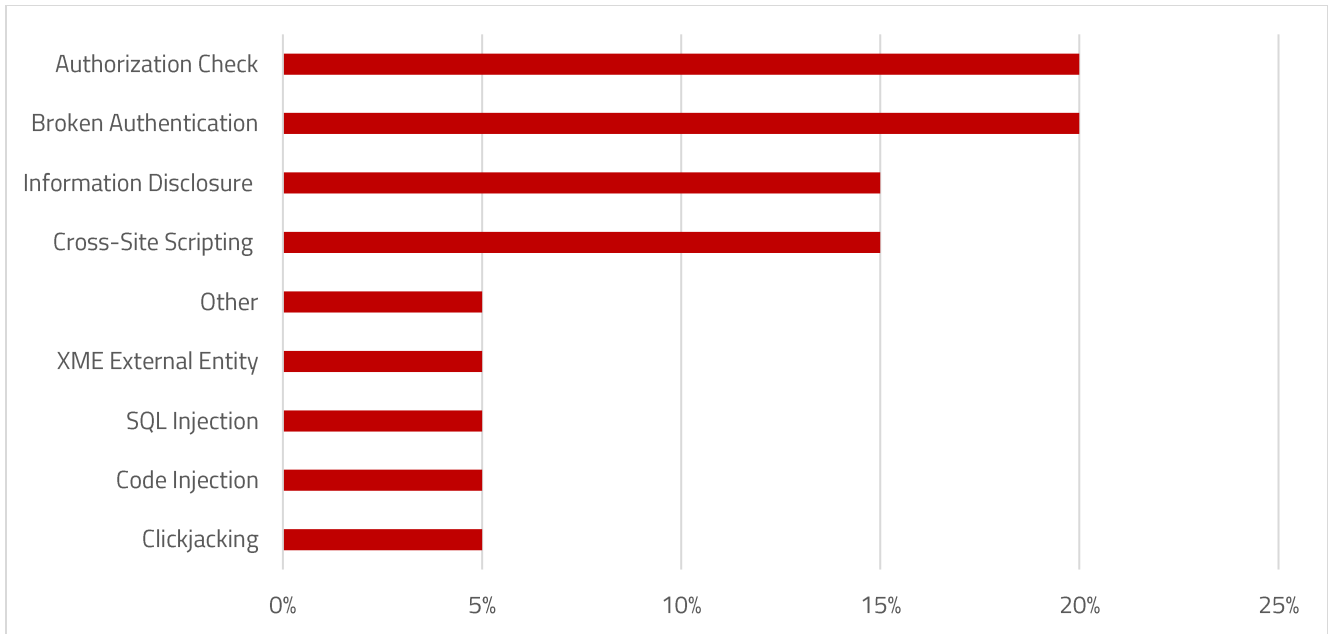
Note 2442993 deals with a high-risk vulnerability in the Host Agent for SAP HANA. The Host Agent is automatically installed with every SAP instance on NetWeaver 7.02 and higher. The stand-alone component is used for controlling and monitoring SAP and non-SAP instances, databases and operating systems. Note 2442993 recommends upgrading to version 7.21 PL25 to remove a vulnerability in earlier versions that could be exploited by attackers to shutdown the Host Agent through malicious SOAP requests used for cross-platform communication via transport protocols such as HTTP and XML. A shutdown of the Host Agent could interrupt the availability of SAP services and explains the high CVSS score of 7.5/10 within the Note. Detailed instructions for upgrading the Host Agent are available in Note 1031096. The command `./saphostexec -upgrade` should be performed after steps 1-4 outlined in the installation section of the Note.

Note 2476601 has an even higher CVSS score of 8.1/10. The note removes missing authentication checks in the SAP Point-of-Sale (POS) Xpress Server. The POS Xpress Server integrates components within the SAP POS suite including applications, clients and databases. Xpress Servers with Internet connectivity are particularly vulnerable to exploits targeting the missing authentication checks patched by the Note.

Note 2478377 recommends upgrading Sybase products impacted by Sweet32 attacks that target design weaknesses in

## SAP Security Notes

July 2017



## SAP Security Notes by Vulnerability Type

some 64-bit block ciphers such as Triple-DES and Blowfish commonly used by the Internet protocols TLS, SSH and IPSec. The Sweet32 attack was discovered by researchers from the French National Research Institute for Computer Science (INRIA) in 2016 and can be used to recover HTTP session cookies in some specific scenarios.

Notes 2100926, 2184221 and 2185122 introduce switchable authorization checks for certain RFC enabled function modules in Business Warehouse, Public Services, and Master Data Governance. Switchable authorization checks supplement checks for the S\_RFC authorization object and should be activated using transaction SACF.

# Appendix: SAP Security Notes, July 2017

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2442993	BC-CCM-HAG	Malicious SAP Host Agent Shutdown without Authentication
HIGH	2476601	IS-R-TGM-POS	Missing Authentication checks in SAP Point of Sale (POS) Retail Xpress Server
HIGH	2416119	BC-JAS-WEB	Improved security for outgoing HTTPS connections in SAP NetWeaver
MEDIUM	2290783	BC-JAS-WEB	Whitelist based Clickjacking Framing Protection for Java Server Pages
MEDIUM	2478964	CRM-ISA	Cross-Site Scripting (XSS) vulnerability in SAP CRM Internet Sales Administration Console
MEDIUM	2458021	BI-BIP-AUT	Information Disclosure vulnerability in LDAP Authentication for SAP BusinessObjects Enterprise
MEDIUM	2453640	GRC-SAC-ARQ	Code Injection vulnerability in Governance, Risk and Compliance Access Controls
MEDIUM	2424742	MDM-FN-CON	Information Disclosure in SAP NetWeaver Master Data Management
MEDIUM	2409262	BI-BIP-LCM	Cross-Site Scripting (XSS) vulnerability in BI Promotion Management Application
MEDIUM	2398144	BI-DEV-WEB	Missing XML Validation vulnerability in SAP Business Objects Titan
MEDIUM	2100926	FIN-SEM-BCS-IS-BW	Switchable authorization checks for RFC in SEM-BCS
MEDIUM	2184221	PSM-FM-CL	Switchable authorization checks for year-end closing transactions
MEDIUM	2218598	FS-MCM-FAC	Additional authorization checks in facilities component
MEDIUM	1568213	CRM-CHM	PCM - Implement enhancement: Restrict Access to WebClient UI
MEDIUM	2158791	EP-KM-WD	Caching KM Content in the Portal
MEDIUM	2088593	LO-MD-BP-CM	Potential disclosure of persisted data in LO-MD-BP-CM & LO-MD-BP-VM
LOW	2478377	BC-SYB-SQA	Exposure to Sweet32 vulnerability in multiple SAP Sybase products
LOW	1920522	SCM-BAS-UIF	Unauthorized modification of stored content in SCM-BAS-UIF
LOW	2459319	BC-MOB-DOE	Weak encryption used in SAP Netweaver Data Orchestration Engine
LOW	2185122	CA-MDG-APP-FIN	Switchable authorization checks for RFC in data extraction within CA-MDG-APP-FIN



Layer Seven Security serve customers worldwide to harden, patch and monitor SAP systems against cyber threats using SAP Solution Manager

**Address**

99 Hudson Street  
5th Floor  
New York, NY 10013  
United States

**Web**

[www.layersevensecurity.com](http://www.layersevensecurity.com)

**Email**

[info@layersevensecurity.com](mailto:info@layersevensecurity.com)

**Telephone**

1-647-964-7370



© Copyright Layer Seven Security 2017 - All rights reserved.

No portion of this document may be reproduced in whole or in part without the prior written permission of Layer Seven Security.

Layer Seven Security offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Layer Seven Security makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.

This publication contains references to the products of SAP AG. 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 AG 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.