Layer Seven Security

ADVISORY

SAP Security Notes

December 2015

SAP Security Notes

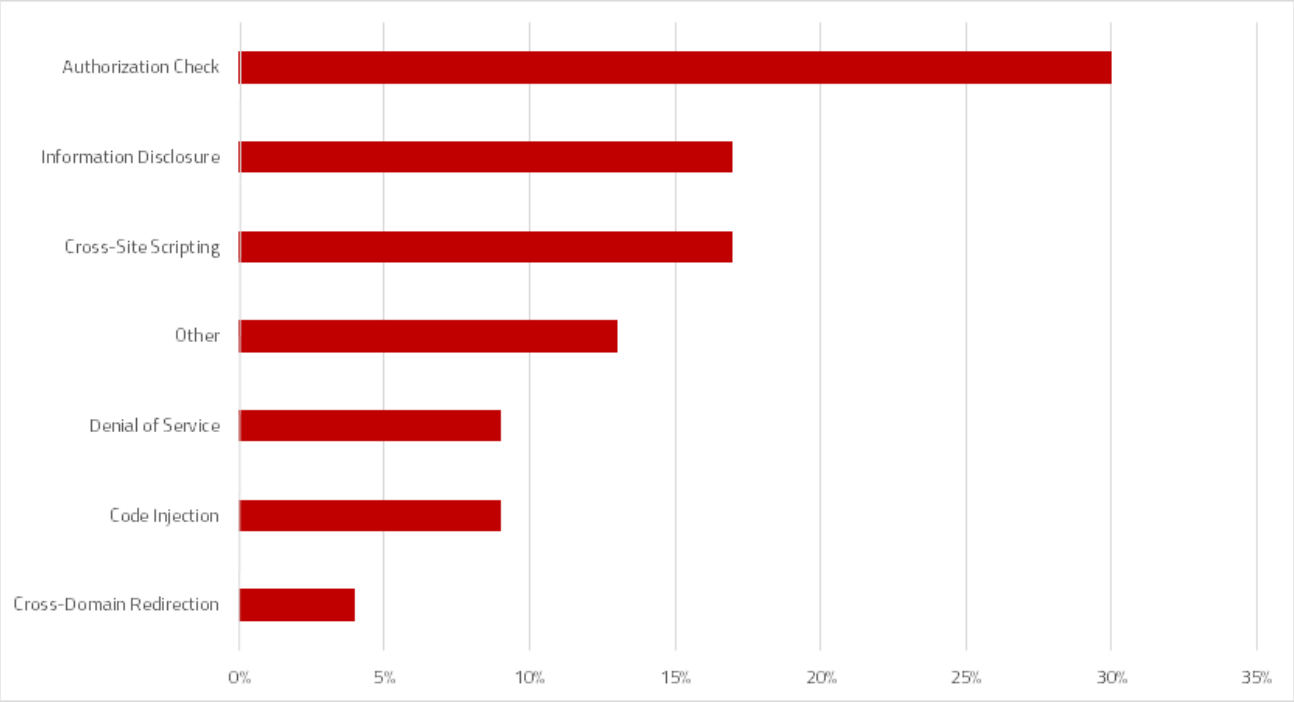
December 2015

SAP released several high priority Notes in December for vulnerabilities impacting components of Business Intelligence. This included areas such as BI Administration, the launch pad, and the Web Application Container Service (WACS). Notes 2117322, 2018683, 2165429, 2168349, 2067570 and 2117322 address vulnerabilities that could be exploited by attackers to discover sensitive information such as server versions, host addresses, server names, and listening ports. The weaknesses could also be exploited to steal user credentials or perform denial-of-service and man-in-the-middle attacks.

Notes 2248862 and 2108479 patch missing authorization checks in critical applications such as invoicing and general ledger accounting in the Financial Accounting (FI) module of ECC. SAP also released patches for missing authorization checks in the Java Application Server (Note 2240946), Business Warehouse (Note 2228520), the Sybase ASE database (Note 2240755) and the Mobile Platform (Note 2227855).

Note 2198151 removes a critical Cross-domain redirection vulnerability that exposes the Internet Communication Manager (ICM) of AS ABAP to phishing attacks. Customers should implement the relevant kernel patches specified in the Note.

Note 2190621 introduces an important new profile parameter to support logging of peer (router) IP addresses in the Security Audit Log. This is preferable to logging client IP addresses since peer IP addresses cannot by manipulated by users. Once the relevant kernel patch is applied, the



SAP Security Notes by Vulnerability Type

parameter rsau/log_peer_address should be set to 1 to record peer IP addresses in log entries.

Finally, Note 2234226 recommends running NetWeaver Search and Classification (TREX) and Business Warehouse Accelerator (BWA) in isolated sub-networks. This is to prevent the execution of remote OS commands on host machines using the rights of the <SID>ADM operating system user. This user has full authorizations for SAP systems and databases.

Appendix: SAP Security Notes, December 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2248673	IS-SE-CCO	Security vulnerabilities found in Apache Groovy Library used in SAP Customer Checkout
HIGH	2204160	CA-UI5-COR	Unauthorized modification of displayed content in SAPUI5
HIGH	2198151	BC-CST-IC	Potential false redirection of web site content in Internet Communication of AS ABAP
HIGH	2117322	BI-BIP-CMC	SAP BusinessObjects WACS is vulnerable to POODLE attacks
HIGH	2240755	BC-SYB-ASE	Missing authorization check in SAP ASE
HIGH	2018683	BI-BIP-ADM	Potential information disclosure relating to BI-BIP
HIGH	2165429	BI-BIP-BIW	Unauthorized modification of displayed content in BI Workspace
HIGH	2168349	BI-BIP-INV	Unauthorized modification of displayed content in InfoView
HIGH	2067570	BI-BIP-ADM	Potential denial of service in BI-BIP
HIGH	2227169	CA-VE-VEV	Potential remote code execution in SAP 3D Visual Enterprise Author, Generator and Viewer
HIGH	2227855	MOB-SUP-SCC	SMP unauthenticated access to SysAdminWebTool servlets
HIGH	2228520	BW-PLA-BPC-ADM	Missing authorization check in BW-PLA-BPC-ADM
HIGH	2234226	BC-TRX	TREX / BWA: Potential technical information disclosure / host OS compromise
MEDIUM	2248862	FI-CAX-INV	Fehlende BerechtigungsprÃ¼fung in FI-CA-INV
MEDIUM	1949253	XX-CSC-RU-FI	Missing authorization check in XX-CSC-RU-FI
MEDIUM	2190621	BC-CST-GW	SAP Netweaver SAL incorrect logging of addresses
MEDIUM	2189178	BI-BIP-SRV	Potential information disclosure relating to BI-BIP-ADM
MEDIUM	2240946	BC-JAS-ADM-LOG	Log Viewer mishandles system credentials
MEDIUM	2238932	MOB-ONP-SEC	Potential modif./disclosure of persisted data in Agentry Server
MEDIUM	2081677	FIN-SEM-CPM	Unauthorized modification of stored content in FIN-SEM-CPM
MEDIUM	2220064	BC-CCM-MON-OS	Potential denial of service in saposcol
MEDIUM	2108479	FI-GL-GL-G	Missing authorization check in FI-GL-GL-G
LOW	2151108	BC-CCM-SLD-REG	SLDREG fixed key for encryption

LAYER SEVEN SECURITY

Layer Seven Security empowers organisations to realize the potential of SAP systems. We serve customers worldwide to secure systems from cyber threats. We take an integrated approach to build layered controls for defense in depth

Address
Westbury Corporate Centre
Suite 101
2275 Upper Middle Road
Oakville, Ontario
L6H 0C3, Canada

Web
www.layersevensecurity.com
Email
info@layersevensecurity.com
Telephone
1 888 995 0993

© Copyright Layer Seven Security 2015 - 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.