Layer Seven Security

ADVISORY

SAP Security Notes

December 2014

SAP Security Notes

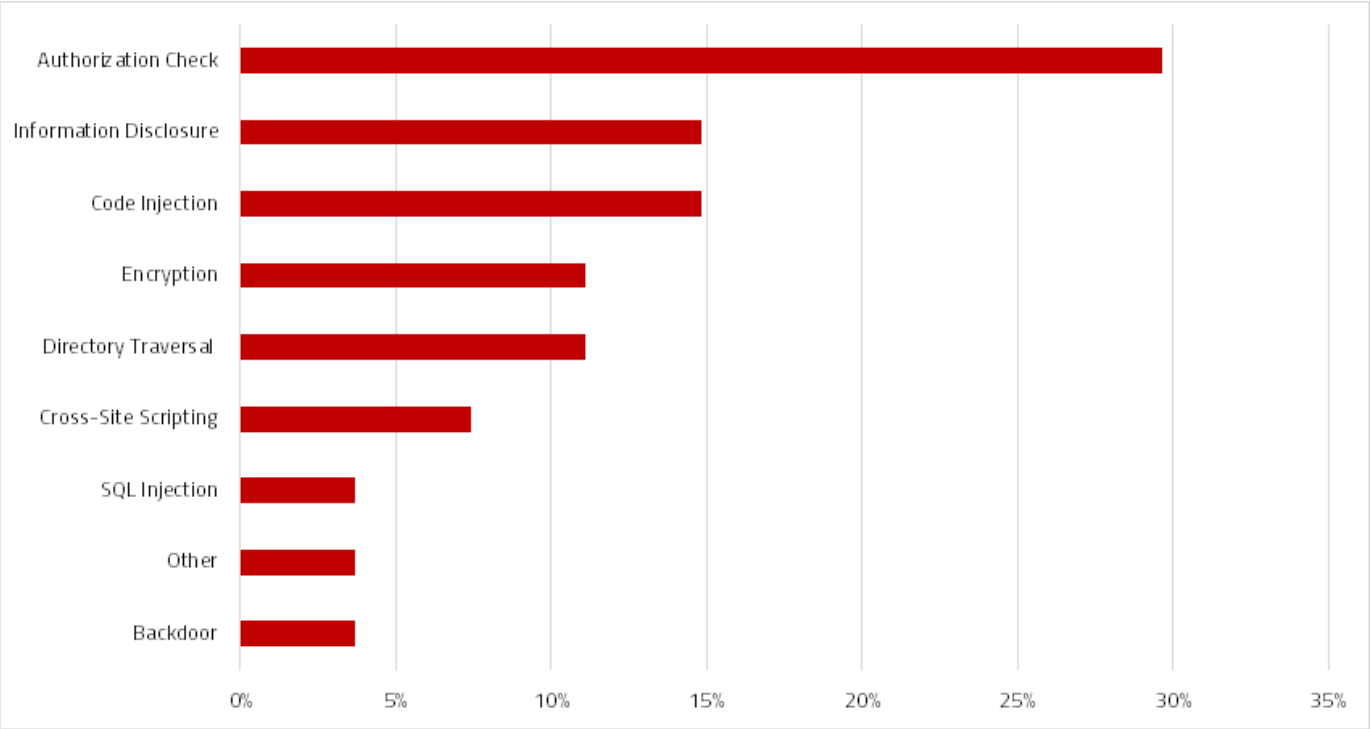
December 2014

SAP issued several more Hot News Notes in December to patch applications and components vulnerable to the POODLE (Padding Oracle On Downgraded Legacy Encryption) man-in-the-middle exploit. This includes the Mobile Money platform of the Sybase Mobiliser solution. The platform drives mobile banking for many financial institutions. Note 2107562 includes instructions for removing support for the vulnerable SSLv3 protocol in the Apache HTTP daemon, Tomcat and other components in Money Mobiliser. Note 2105763 recommends upgrading the Agentry Server of the SAP Mobile platform to remove the POODLE vulnerability.

Note 2059734 includes a kernel patch to remove a dangerous buffer overflow vulnerability impacting batch management functions used to import and process large volumes of data. The vulnerability could be exploited to provoke a denial of service or assume control of the impacted component through the processing of malicious code injected into working memory. The sequence of transactions impacted by the vulnerability include the Batch Input Transaction Recorder (SHDB) and Batch Input Monitoring (SM35).

Note 2061271 deals with a similar buffer overflow exploit in the host spool system (BC-CCM-PRN). This is an operating system spooler that receives print data from the SAP spool system.

Note 2102941 includes updated corrections for controlling RFC callbacks. RFC callbacks enable servers to open RFC connections in clients during synchronous calls using the privileges of the RFC user in the client system. This can pose a serious security risk, especially when destinations are configured with privileged users and the callback establishes a connection from a system with a lower trust level. For systems with SAP Basis 7.0+ and kernel 7.21+, the Note recommends configuring positive whitelists for permitted callbacks using transaction SM59. The profile parameter rfc/callback_security_method should be set to 3



SAP Security Notes by Vulnerability Type

to enforce the whitelists after an appropriate simulation phase to identify required callbacks. During the simulation phase, successful and unsuccessful callbacks can be identified in the Security Audit Log through the DUI and DUJ event logs. Systems with SAP Basis 6.20 and 6.40 with kernel 6.40 or SAP Basis 7.00 – 7.31 with kernel 7.20 do not support whitelists for callbacks. For these systems, the Note recommends controlling RFC callbacks directly in the program code by implementing the function module RFC_CALLBACK_REJECTED RFC.

Other critical Notes released in December include 2087906 and 2051285. Note 2087906 deals with a hardcoded user and therefore a potential backdoor in the ECATT_ESF_RECORDING function module within the eCATT Extended Computer Aided Test Tool. eCATT can provide full access to the application and database layers in SAP systems for functional testing.

Note 2051285 patches a non-persistent reflected cross-site scripting vulnerability in the Netweaver Business Client for HTML 3.0 when used with SAP Basis 720. The vulnerability can be exploited to steal authentication data and should be removed by deactivating NWBC nodes using transaction SICF.

Appendix: SAP Security Notes, December 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2107562	MOB-MCO-MM	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability in Money Mobiliser Platform
HOT NEWS	2092489	BC-SEC	update to note 2067859
HOT NEWS	2105793	MOB-SYC-SAP	Fixing Poodle SSLv3 vulnerability for Agentry
HIGH	2059734	BC-ABA-SC	Potential remote code execution in ABAP VM
HIGH	2058866	IS-R-PUR-AHD	Potential modification of persisted data in IS-R-PUR-AHD
HIGH	1950021	BC-WD-ABA	Missing authorization check in Web Dynpro ABAP
HIGH	2051285	BC-FES-BUS	Unauthorized modification of displayed content in Netweaver Business Client for HTML 3.0
HIGH	2048266	SV-SMG-SDD	Missing authorization check in SV-SMG-SDD
HIGH	1987344	BC-UPG-OCS	Code injection vulnerability in the OCS functionality (Support Package Manager / Add-On Installation Tool)
HIGH	1838854	BC-ABA-TO	Missing authorization check in ABAP Report Variants
HIGH	2091973	FS-CD	Missing authorization check in FS-CD
HIGH	2087906	BC-TWB-TST-ECA	Hard-coded credentials in BC-TWB-TST-ECA
HIGH	2077260	IM-FA-IS	Directory traversal in IM summarization reporting
HIGH	2071329	IS-A-DP	Update 1 to security note 1676754
HIGH	2061271	BC-CCM-PRN-SPO	Potential remote code execution in spool.
HIGH	2101271	XX-CSC-BE	Update 1 to security note 1533533
HIGH	2102941	BC-MID-RFC	Update 1 to Security Note 1686632
MEDIUM	2069588	FIN-FSCM-BD-AR	Switchable authorization checks for RFC in Biller Direct
MEDIUM	1783807	CA-CL-SEL	Missing authorization checks in CA-CL
MEDIUM	2057277	BC-SYB-SQA	Potential exploit in SAP SQL Anywhere ADO.Net driver
MEDIUM	2056333	IS-ADEC-SPC	Directory traversal in IS-ADEC-SPC
MEDIUM	2055411	CRM-ISA-TEC	Potential information disclosure relating to E-Commerce/Web Channel
MEDIUM	2048335	EP-KM-CM-UI	Potential information disclosure relating to KM Content
MEDIUM	2038190	MOB-SYC-SAP	Potential information disclosure relating to the Agentry 6.1.3 iOS Client
MEDIUM	1640531	BC-MID-RFC	Protecting data against change to destination authorization
MEDIUM	2068191	MOB-AFA	Potential information disclosure relating to device notification details in Afaria Server
MEDIUM	2024328	BC-JAS-COR	Missing authorization check in AS Java

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 2014 - 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.