ADVISORY

Layer Seven Security

SAP Security Notes

November 2014

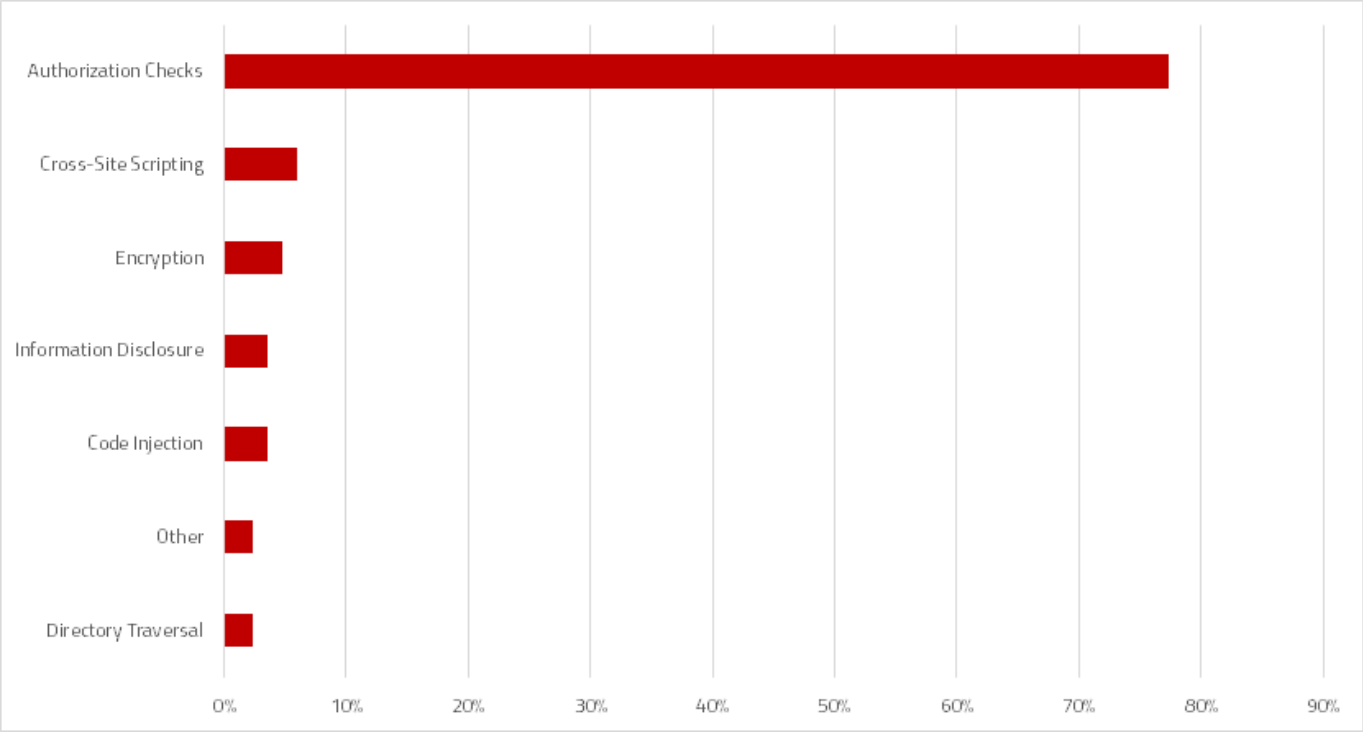
SAP Security Notes

November 2014

SAP issued a total of 84 Security Notes in November. Approximately half were Support Package Notes providing switchable authorization checks for function modules in specific application components. Switchable authorization checks can significantly improve S_RFC authorization checks for remote-enabled function modules but are inactive by default to prevent interruptions to existing business operations. They can be activated for the authorization scenarios delivered in the SAP Notes using the switchable authorization check framework (transaction SACF). Administrators should use SACF to identify users that require the new checks before activation. Check results are written to the security audit log and can be viewed in the DUO and DUQ event logs, accessible through transaction SM20 and the report RSAU_SELECT_EVENTS. The additional authorizations should be included in the roles assigned to the users identified in the logs before activating the checks.

The Support Package Notes issued by SAP in November deliver additional authorization checks for critical function modules in applications and areas such as Public Sector Contract Accounting and Procurement, CRM, Funds Management, and Sales and Distribution. Some of the function modules can be used to access and modify banking, billing, customer and other types of sensitive data. Therefore, the implementation of the relevant Support Packages is highly recommended.

SAP also released a batch of Notes to patch Sybase, Afaria, Business Intelligence, HANA and other products, as well as both the NetWeaver Application Server ABAP and Java, impacted by the POODLE vulnerability. The vulnerability exposes systems to man-in-the-middle attacks that could lead attackers to decrypt communications traffic encrypted using the insecure SSL 3.0 protocol. Notes 2096275, 2094995, 2089135 and 2086818 address the vulnerability by removing client and server side support for the protocol.



SAP Security Notes by Vulnerability Type

Note 2074889 introduces a kernel patch for releases 720 and 721 to address a critical vulnerability in the message server that carries the highest possible CVSS score of 10.0. The patch is an update for Note 1800603 released in January 2013. The message server is a core communications hub in SAP landscapes, managing data exchange and load balancing between systems. Notes 2074889 and 1800603 correct a buffer overflow vulnerability that could lead attackers to take complete control over the message server through the injection of malicious code.

Note 1738988 also addresses a critical code injection vulnerability impacting the ABAP dictionary used to manage metadata in SAP systems including objects such as domains, types, tables and table groups known as views. The correction instructions delivered through the Note restrict ABAP Dictionary functions performed through the report RADGENREP. This includes executing user-defined code that could be used to access and modify sensitive data, create users with elevated privileges or perform a denial of service attack.

Finally, Note 2046493 recommends disabling s-bit for saposcol in Unix platforms. Saposcol is a stand-alone component used to collect host-level data such as memory, CPU and disk usage which is read by the CCMS agent. S-bit is often used to control the ability of users to delete files in directories, especially public directories. However, it can lead to a privilege escalation vulnerability if set on the saposcol directory.

Appendix: SAP Security Notes, November 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2096275	BC-SYB-SQA	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability in multiple SAP Sybase products
HOT NEWS	2094995	MOB-AFA	Afaria Server Poodle Mitigation
HOT NEWS	2089135	SBO-BC	Upgrade OpenSSL to resolve the POODLE issue with the SSL 3.0 protocol
HOT NEWS	2086818	BC-SEC-SSL	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability
HOT NEWS	2074889	BC-CST-MS	Update 1 to security note 1800603
HIGH	2058959	BC-MOB-MI-SER	Missing authorization check in BC-MOB-MI-SER
HIGH	2054613	BC-MID-RST	Missing authorization check in ODATA-CXF-EXT
HIGH	2046493	BC-CCM-MON-OS	Privilege escalation vulnerability in saposcol
HIGH	2039348	GRC-ACP	Missing whitelist check in GRC-ACP
HIGH	2037976	IS-A-ESD	SACO: No authorization check on Sales Organization
HIGH	2037572	BC-CCM-ADK	Update 1 to security note 1486309
HIGH	2010819	CA-UI5-TOL	Unauthorized modification of displayed content in UI_INFRA and SAP_UI
HIGH	1738988	BC-DWB-DIC-AC	Code injection vulnerability in ABAP Dictionary
HIGH	1972093	BI-BIP-AUT	Untrusted XML input parsing possible in BI4
HIGH	1922183	BC-XI-CON-SOP	Modification of displayed content in XI SOAP Adapter
HIGH	2074736	BC-CST-GW	Directory traversal in GW
HIGH	2072813	BC-CCM-MON	Missing authorization check in BC-CCM-MON
HIGH	2070691	SV-SMG-SDD	Potential information disclosure relating to database server file system
MEDIUM	1922485	EHS-SAF-RCK	Missing whitelist check in EHS-SAF-RCK and EHS-BD-TLS
MEDIUM	2030144	IS-HER-CM	Switchable authorization checks for RFC in SLCM(Student Life cycle Management)
MEDIUM	2030096	LO-SRS	Missing authorization check in component LO-SRS
MEDIUM	2029561	IS-OIL	Missing Auth. Check in IS-OIL
MEDIUM	2029526	CA-CL	Missing authorization check in CA-CL
MEDIUM	2030357	IS-A-LMN	Switchable authorization checks for RFC in Material Version
MEDIUM	2029397	CRM-ISA-R3	Missing authorization checks for RFC in E-commerce ERP applications

Appendix: SAP Security Notes, November 2014

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2029077	FI-FM	Switchable authorization checks for RFC in FI-FM and PSM-FM
MEDIUM	2028559	IS-A	RFC Missing authorization check in IS-A
MEDIUM	2028525	FI-LA	Missing authorization check in FI-LA
MEDIUM	2028501	PP-SFC-EXE-CON	Missing authorization check in PP-SFC-EXE-CON
MEDIUM	2027797	IS-DFS-MA	Missing Authority Check in Mobile Defense RFC function modules
MEDIUM	2027715	FI-CAX	Switchable authorization checks for RFC in FI-CAX
MEDIUM	2027682	CS-SE-FS	EAM: RFC capability in component CS-SE-FS
MEDIUM	2027145	LO-MD-MG	Missing authorization check in LO-MD-MG
MEDIUM	2026939	IS-U	Switchable authorization checks for RFC in IS-U
MEDIUM	2026641	FS-CD	Switchable authorization checks for RFC in FS-CD
MEDIUM	2026528	PM	EAM: RFC capability: Function module F4_FILENAME_SERVER
MEDIUM	2026361	LE-DSD	Missing authorization check in LE-DSD and SD-SLS-PLL
MEDIUM	2059230	PA-ER	Authorization checks for RFC in E-Recruiting
MEDIUM	2059285	LO-MD-BP-CM	Switchable authorization checks for RFC in LO-MD-BP-CM
MEDIUM	2058934	LE-WM	Switchable authorization checks for RFC in LE-WM
MEDIUM	2054064	CA-GTF-DOB	Missing authorization check in CA-GTF-DOB.
MEDIUM	2052113	CRM-MW-ADP	Switchable authorization checks for RFC in CRM-MW-ADP
MEDIUM	2049681	CRM-MKT-MPL-ST-ERP	Authorization checks for RFC in CRM-MKT-MPL-ST-ERP
MEDIUM	2046243	PA-PA-XX	Switchable authorization checks for RFC in Payroll, Time Management and ESS/MSS (SAP_HR)
MEDIUM	2045668	EP-KM-TLS-XFB	Potential information disclosure relating to XMLForms
MEDIUM	2044543	BC-BMT-OM	Switchable authorization checks for RFC in Workflow and ESS
MEDIUM	2038210	FIN-FSCM-IHC	Switchable authorization checks for RFCs in In House Cash
MEDIUM	2032723	SRM-EBP-INT	Switchable authorization checks for RFC in SRM
MEDIUM	2031795	IS-R-PUR-MPO	Missing authorization check in IS-R-PUR-MPO
MEDIUM	2030997	FI-AP-AP	Switchable authorization checks for RFC in FI-AP-AP
MEDIUM	2030657	PSM-GPR	Switchable authorization checks for RFC in PSM-GPR

Appendix: SAP Security Notes, November 2014

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2030674	IS-A	Enforcing internal RFC in IS-A
MEDIUM	2066956	EHS-SAF	Switchable authorization checks for RFC in EHS
MEDIUM	2066023	SD-EDI	Switchable authorization checks for RFC in SD
MEDIUM	2064637	LO-MD-PL	Switchable authorization checks for listing and site master data
MEDIUM	2064048	LO-SPM	Switchable authorization checks for RFC in LO-SPM
MEDIUM	2063792	LO-AB	Missing authorization check in LO-AB
MEDIUM	2062526	CRM-MD-BP-IF	Missing authorization check in CRM-MD-BP-IF
MEDIUM	2062186	BC-BMT-OM	Switchable authorization checks for RFC in ESS_USERS_OF_ROLE_GET
MEDIUM	2061519	IS-M	Switchable authorization checks for RFC in IS-M, part 2
MEDIUM	2024225	CO-OM	Switchable authorization checks for RFC in CO-OM and CO-PA
MEDIUM	2023693	SD-BIL	Switchable authorization checks for RFC in SD
MEDIUM	2023449	FI-AR-AR	Switchable authorization checks for RFC in FI, FI-AP-AP, FI-AR-AR, FI-BL-MD-BK
MEDIUM	2023335	CA-JVA	Switchable authorization checks for RFC in CA-JVA
MEDIUM	2023207	IS-T-CA	Switchable authorization checks for RFC in IS-T-CA
MEDIUM	2022888	IS-M	Switchable authorization checks for RFC in IS-M
MEDIUM	2022818	FS-CML	Authorization check for RFC in FS-CML
MEDIUM	2018479	BC-FES-IGS	Potential remote code execution due to buffer overflow in libtiff
MEDIUM	2013153	EHS-BD	Switchable authorization checks for RFC in Environment, Health & Safety
MEDIUM	1988565	IS-B-BCA-MD	Switchable Authorization Checks for RFC in IS-B-BCA
MEDIUM	2025974	LO-BM	Missing authorization checks in LO-BM
MEDIUM	2025794	CA-MDG-APP-ISS	Missing authority check in CA-MDG-APP-ISS
MEDIUM	2025390	IS-DFS-BIT-DIS	Missing authorization check in function module /ISDFPS/ ALE_SET_SYSTEM_STATE
MEDIUM	2078596	BC-MID-RFC	Further improvements for RFC security
MEDIUM	2072641	IS-H	Authorization checks for RFC in Patient Register
MEDIUM	2071371	XAP-MBA-DSD	Missing authorization check in XAP-MBA-DSD

Appendix: SAP Security Notes, November 2014

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2071323	EPM-BFC-TCL	Unauthorized modification of displayed content in Financial Consolidation 10.0
MEDIUM	2069864	CA-BK	Switchable authorization checks for RFC in the IBAN maintenance
MEDIUM	2068606	CRM-BE	Switchable authorization checks for RFC in LO
MEDIUM	1687863	PPM-PFM	Unauthorized Access of document possible in PPM-PFM
MEDIUM	1731835	PPM-PFM	Unauthorized modification of displayed content in PPM-PFM
LOW	2073000	CRM-IC-FRW	Potential information disclosure relating to UserID
LOW	2031117	PLM-RM	Missing authorization check in PLM-RM-TRL
LOW	1995783	AP-PRC-PR	Authority check for remote enabled Function Module SELECT_COUNT

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