ADVISORY

Layer Seven Security

SAP Security Notes

September 2017

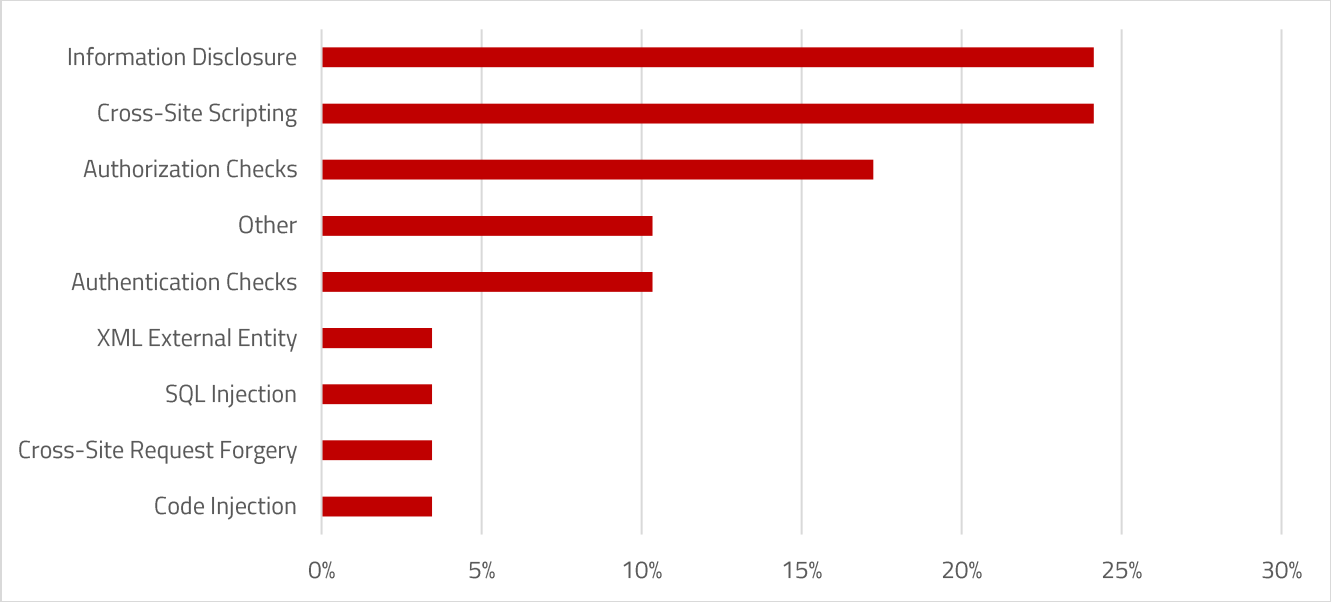
SAP Security Notes

September 2017

Note 2408073 prepares systems to handle digitally signed SAP Notes. Digitally signed Notes will be issued by SAP in the future to protect against the risk of uploading Notes containing malware. Digital signatures will support authentication and the identification of changes performed by attackers to SAP-delivered Notes. SAP recommends only uploading digital signed Notes once they are available.

Note 2518518 should be implemented before Note 2408073 to install new objects required to support Notes with digital signatures. The Notes will update the Note Assistant tool to verify digital signatures using the SAPCAR utility. SAPCAR must version 7.20, patch level 2 or higher. The Note Assistant tool will process ZIP files containing Notes downloaded from the SAP Support Portal and log the results of digital signature checks. Notes that fail the digital signature check will be logged in the Application Log (transaction SLG1) and read by the Notes Assistant using the authorization object S_APPL_LOG. For further information, refer to 2537133 – FAQ – Digitally Signed SAP Notes and the Digital Signature User Guide referenced in Note 2408073.

Note 2520064 provides detailed instructions for removing a missing authentication check in the SAP Point-of-Sale (POS) Retail Xpress Server that was originally reported in July. The vulnerability could be exploited by attackers to modify files, capture sensitive information and perform a denial of service.



SAP Security Notes by Vulnerability Type

Notes 2531241 and 2520772 provide corrections for patching SAP Landscape Management (LVM) to prevent the storage of sensitive information including administrative passwords in plaintext within logs that can be read in database tables. The patches released with the Notes prevent LVM from persisting passwords in plaintext but do not remove sensitive information already stored in the logs. Therefore, the solution section includes instructions for changing passwords and discovering and removing sensitive log entries.

Finally, Note 2278931 removes a high-risk code injection vulnerability in Document Management Services. The vulnerability could be exploited by attackers to create backdoors or escalate privileges.

Appendix: SAP Security Notes, September 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2531241	BC-VCM-LVM	Disclosure of Information/Elevation of Privileges LVM 2.1 and LaMa 3.0
HIGH	2520772	BC-VCM-LVM	Disclosure of Information/Elevation of Privileges LaMa 3.0
HIGH	2278931	BC-SRV-KPR-DMS	Code injection vulnerability in BC-SRV-KPR-DMS
HIGH	2367269	XX-PROJ-CDP-354	Cross-Site Request Forgery (CSRF) vulnerability in Electronic Ledger Management for Turkey 1.0
HIGH	2476601	IS-R-TGM-POS	Missing Authentication checks in SAP Point of Sale (POS) Retail Xpress Server
HIGH	2520064	IS-R-TGM-POS	Missing Authentication check in SAP Point of Sale (POS) Retail Xpress Server
MEDIUM	2531131	FI-CAX-FS	Switchable Authorization checks for RFC BCA_DIM_WRITE_OFF in Loans (FI-CAX-FS)
MEDIUM	2507798	PA-ER	Bypass of email verification in e-recruiting
MEDIUM	2389764	BW-BEX-OT-WSP	BW Workspaces: Analysis authorization during modeling and running local hierarchies
MEDIUM	2044018	BW-SYS-DB	Missing authorization check in BW-SYS-DB
MEDIUM	2051717	BC-CCM-MON-ORA	SQL injection vulnerability in SAP NetWeaver
MEDIUM	2492658	EP-BC-UWL	Missing XML Validation vulnerability in SAP NetWeaver Java Workflow (JWF)
MEDIUM	2365450	SLC-REG	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver SLC Sell Side Registration Page
MEDIUM	2484707	MOB-APP-BI-IOS	Multiple vulnerabilities In SAP BI mobile application
MEDIUM	2408073	BC-UPG-NA	Handling of Digitally Signed notes in SAP Note Assistant
MEDIUM	2491480	BC-WD-JAV	Cross-Site Scripting (XSS) vulnerability in SAP Netweaver Portal
MEDIUM	2489196	BC-TRX	Information Disclosure in TREX / BWA
MEDIUM	2488516	BC-WD-ABA	Cross-Site Scripting (XSS) vulnerability in Web Dynpro ABAP
MEDIUM	2471209	BC-FES-ITS	Cross-Site Scripting (XSS) vulnerability in SAPGUI for HTML
MEDIUM	2469860	BC-WD-UR	Cross-Site Scripting (XSS) vulnerability in Web Dynpro Java

Appendix: SAP Security Notes, September 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2464489	BI-BIP-BIW	Cross-Site Scripting (XSS) vulnerability in BI Workspace
MEDIUM	2444673	BC-CTS-DI	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Development Infrastructure Cockpit
MEDIUM	2342974	XX-PART-ADB-IFM	Arbitrary Valid Certificate Vulnerability in Adobe Document Services
MEDIUM	2261768	CRM-MW-ADM	Switchable authorization checks for RFC in CRM-MW-ADM
MEDIUM	2520885	SV-RDS-PAK	Logout function missing in SAP Best Practices Package Manager for Partner
MEDIUM	2432578	IS-U-LIB-DE-CL	Missing authorization check in RFC function module
MEDIUM	2296722	BC-SYB-ASE	Information Disclosure vulnerability in SAP ASE Installer
LOW	2483143	BC-NWA-XPI	Information Disclosure in SAP NetWeaver Adapter Engine Cache Monitor
LOW	2374348	BC-SYB-SQA	Information Disclosure in DBISQL affecting SAP SQL Anywhere, SAP ASE and SAP IQ

LAYER SEVEN SECURITY

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

Email

info@layersevensecurity.com

Telephone

1-647-964-7370