Layer Seven Security

ADVISORY

SAP Security Notes

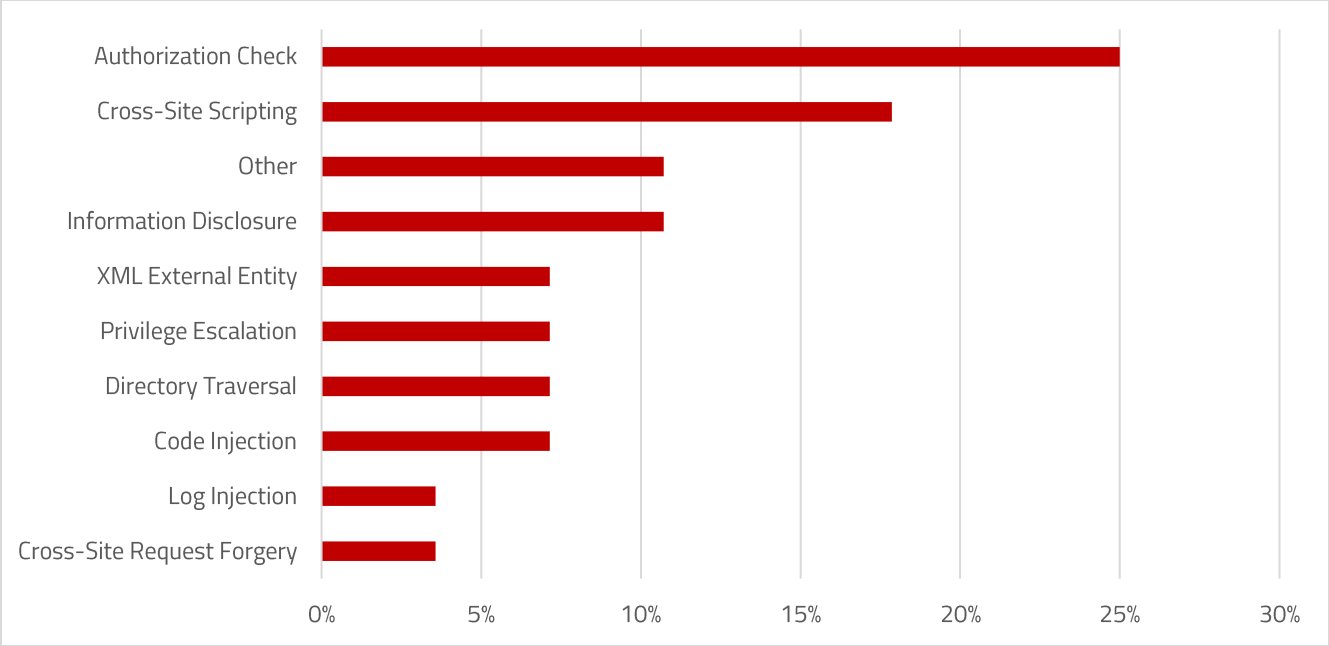
November 2017

Hot News Note 2357141 includes updated instructions for removing a critical OS command injection vulnerability in Report for Terminology Export. This is a component of the Basis area Terminology and Glossary (transaction STERM) used to maintain standard terminology for management reporting, financial controlling, product development, and other areas. Report for Terminology Export does not sufficiently validate user input that is used to perform operating commands through the command variable in system calls. The vulnerability could be exploited to perform arbitrary OS commands using the privileges of the underlying service. This could compromise the SAP file system.

SAP updated the priority of Notes 2531241 and 2520772 from High to Hot News based on revised CVSS scores. The Notes were originally released in September and 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 sections includes instructions for changing passwords and discovering and removing sensitive log entries.

SAP Security Notes

November 2017



SAP Security Notes by Vulnerability Type

Note 2500044 introduces improved key management procedures through the profile variable jstartup/secure_key in order to prevent attackers from accessing private keys used for instance communication in the J2EE.

Note 2026174 deals with a high risk code injection vulnerability in a component of the Apache Struts framework used by SAP BusinessObjects Enterprise.

Finally, Note 2542426 provides recommendations for removing a privilege escalation vulnerability in the Image Imports component of SAP Assortment Planning.

Appendix: SAP Security Notes, November 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2357141	BC-DOC-TER	OS Command Injection vulnerability in Report for Terminology Export
HOT NEWS	2531241	BC-VCM-LVM	Information Disclosure in LVM 2.1 and LaMa 3.0
HOT NEWS	2520772	BC-VCM-LVM	Information Disclosure in LaMa 3.0
HIGH	2026174	BI-BIP-INV	SBOP solution for Apache Struts1.x Vulnerability CVE-2014-0094
HIGH	2500044	BC-JAS-SF	Full access to SAP Management Console
HIGH	2542426	CA-DDF-RT-IF	Missing Authorization check in Image Imports
MEDIUM	2455452	PP-MRP	Missing Authorization check in production planning
MEDIUM	2408073	BC-UPG-NA	Handling of Digitally Signed notes in SAP Note Assistant
MEDIUM	2492999	PE-LSO-CP	Multiple security vulnerabilities in SAP ERP Learning Solution Content Player
MEDIUM	2508673	BC-XS-RT	Information Disclosure in SAP HANA Extended Application Services (XS Advanced)
MEDIUM	2541610	CA-WUI-UI-TAG	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2535629	BC-FES-INS	DLL preload attack possible on NwSapSetup and Installation self extracting program
MEDIUM	2374767	CA-UI5-COR	Cross-Site Scripting (XSS) vulnerability in SAPUI5
MEDIUM	2546220	BC-UPG-NA	SNOTE: Digital signature verification along with note file extraction
MEDIUM	2514475	MOB-APP-BI-SRV	Directory Traversal vulnerability in SAP BI Mobile Server
MEDIUM	2464582	EP-KM-TLS-XFB	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Knowledge Management XMLForms
MEDIUM	2508767	BC-ABA	Privilege Escalation after installation of SAP Systems on SAP HANA
MEDIUM	2493171	BC-CCM-MON	Information Disclosure in SAP NetWeaver Instance Agent Service
MEDIUM	2485208	BC-JAS-SEC	Log Injection Vulnerability in SAP NetWeaver AS Java
MEDIUM	2473504	BI-RA-AWB	Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Analysis Edition for OLAP

Appendix: SAP Security Notes, November 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2545530	BW-WHM-DBA-MD	InfoObject master data maintenance, hierarchy maintenance: CSV export can result in execution of commands in Microsoft Excel
MEDIUM	2469849	XX-CSC-BR-REP	Missing Authorization check in XX-CSC-BR-REP
MEDIUM	1560538	SCM-APO-INT	Missing authorization check in SCM-APO-INT
MEDIUM	2270084	CRM-MW-MFW	Switchable authorization checks for RFC in CRM-MW-MFW
MEDIUM	2264976	CRM-MW-BDM	CRM_Switchable authorization checks for RFC in CRM-MW-BDM
MEDIUM	2328182	CA-MDG-ML	Directory Traversal vulnerability in MDG Data Export
MEDIUM	2400292	BC-DWB-JAV-CAF	Missing XML Validation vulnerability in TranslationSupport application
MEDIUM	2372301	BC-DWB-JAV-CAF	Missing XML Validation in Composite Application Framework Authorization Tool

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