LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

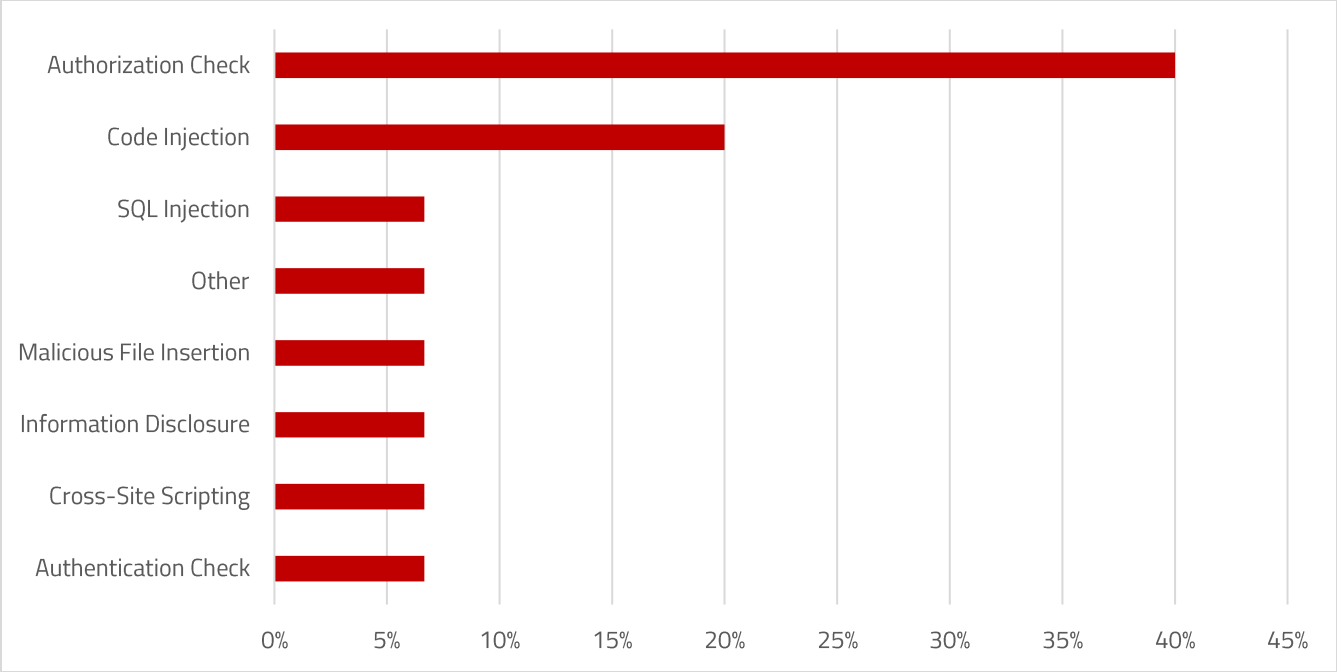
January 2018

Note 2580634 provides instructions for removing a malicious file insertion vulnerability in the Process Control and Risk Management applications of SAP Governance, Risk and Compliance (GRC). The vulnerability could be exploited to upload malicious scripts or other forms of malware to SAP servers. The note includes manual instructions for implementing package GRFN_DOCUMENT_ WT_CHECK of the BAdI GRFN_DOCUMENT. This will activate a positive whitelist in table GRFNDOCUMENTWT to control permitted file extensions and mime types.

Note 2408073 provides updated instructions for the handling of digitally signed notes in the Note Assistant. 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.

SAP Security Notes

January 2018



SAP Security Notes by Vulnerability Type

Note 2507934 provides instructions for adjusting role SAP_BPO_CONFIG in SAP Solution Manager 7.2. The instructions restrict authorizations for table maintenance in the role to BPO-relevant tables belonging to the authorization groups SS, LMDB, PIMA, SA, IWAD, and SC.

Appendix: SAP Security Notes, January 2018

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2512244	FIN-FSCM-TRM-TM-TR	Missing authorization check in Transaction Management
MEDIUM	2580634	GRC-RM	Unrestricted File Upload vulnerability in GRC-PC / GRC-RM
MEDIUM	2579693	BC-ABA-SC	Missing Authorization check in Dynpro Processing
MEDIUM	2427949	LO-MD-BP-CM	Incorrect Authorization Checks in SAP ERP Logistics Customer Master and Vendor Master
MEDIUM	2408073	BC-UPG-NA	Handling of Digitally Signed notes in SAP Note Assistant
MEDIUM	2471736	IS-HER-CM	Switchable Authorization checks for RFC in Accounts in SLcM
MEDIUM	2533541	BC-MID-RST	SQL Injection vulnerability in Olingo JPA
MEDIUM	1906212	BC-SRV-KPR-DMS	Code Injection vulnerability in Knowledge Provider.
MEDIUM	2278931	BC-SRV-KPR-DMS	Update 1 to 1906212: Code injection vulnerability in Knowledge Provider.
MEDIUM	2525392	BC-SRV-KPR-DMS	[CVE-2018-2363] Update 2 to 1906212: Code injection vulnerability in Knowledge Provider.
MEDIUM	2523961	BC-CST-STS	[CVE-2018-2360] Missing Authentication check in Startup Service
MEDIUM	2575750	HAN-DB	[CVE-2018-2362] Information Disclosure in Startup Service in SAP HANA
MEDIUM	2507934	SV-SMG-MON-BPM	[CVE-2018-2361] Improper Role Authorizations in SAP Solution Manager 7.2
MEDIUM	2455452	PP-MRP	Missing Authorization check in production planning
LOW	2453871	BI-RA-AD	Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Design Studio

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