Layer Seven Security

ADVISORY

SAP Security Notes

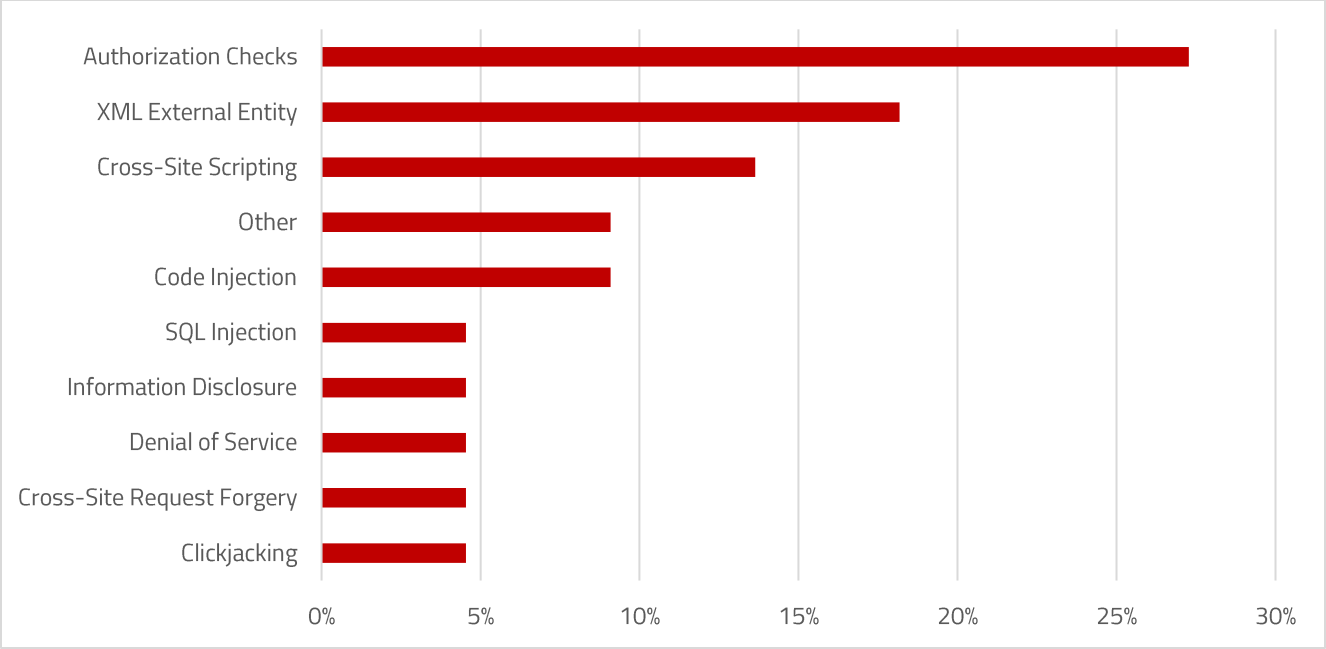
April 2017

SAP Security Notes

April 2017

Hot News Note 2419592 includes further corrections for a code injection vulnerability in TREX that was originally patched by SAP through Note 2234226 in February 2016. The vulnerability impacts the TREXNet protocol used for internal communications by TREX components and servers. TREXNet communication does not require any authentication. Therefore, the protocol can be abused to execute dangerous commands including OS commands using the administrative privileges of the <SID>ADM user. As a result, SAP recommends running TREX in an isolated subnet. Detailed instructions are documented in the TREX Installation Guide. However, the corrections included in Note 2419592 block access to the TREXNet interface from outside the TREX landscape. Therefore, it protects unsegmented systems against malicious commands targeting the protocol. TREX versions 7.10 and 7.25 must be upgraded to revisions 74 and 37 respectively to apply the corrections.

Note 2235515 includes an important update for SNOTE to log information related to the RFC destination used to download notes. SNOTE can be abused to download malicious packages from attacker controlled servers if the default RFC destination is changed. SNOTE executes program SCWN_NOTE_DOWNLOAD during runtime. The program will use an alternative RFC destination maintained in table CWBRFCUSR if a destination is defined in the table. For more information refer to Note 2235514.



SAP Security Notes by Vulnerability Type

Notes 2410082, 2372301, 2400292 and 2387249 deal with weaknesses in XML input validation that expose several ABAP and Java applications to XML External Entity (XXE) attacks. The impact of successful XXE exploits include sensitive information disclosure and denial of service.

Finally, Note 2407616 provides an update for saprules.xml to secure against a high-risk vulnerability that could enable attackers to execute remote commands against SAP GUI. saprules.xml is used by the SAP GUI Security Module to protect clients against potentially malicious commands from back-end SAP servers.

Appendix: SAP Security Notes, April 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2235515	BC-UPG-NA	Insufficient logging in SNOTE
HOT NEWS	2419592	BC-TRX	Code Injection vulnerability in TREX / BWA
HIGH	2421287	BC-CCM-PRN	Security vulnerabilities in SAPLPD
HIGH	2410082	BC-WD-CLT-FLX	Missing XML Validation vulnerability in Web Dynpro Flash Island
HIGH	2407616	BC-FES-GUI	Remote Code Execution vulnerability in SAP GUI for Windows
MEDIUM	2423486	BC-DB-DBI	Missing Authorization check in SAP NetWeaver ADBC Demo Programs
MEDIUM	2142551	BC-WD-ABA	Whitelist service for Clickjacking Framing Protection in AS ABAP
MEDIUM	1791940	IS-DFS-MA	Potential modification of persisted data in MDS
MEDIUM	1830630	IS-HER-CM	Unauthorized modification in BSP application in IS-HER-CM
MEDIUM	1959110	XX-CSC-CL-FI	Missing authorization check in Chile Sales Ledger
MEDIUM	2427949	LO-MD-BP-CM	Incorrect Authorization Checks in SAP ERP Logistics Customer Master and Vendor Master
MEDIUM	2372301	BC-DWB-JAV-CAF	Missing XML Validation in Composite Application Framework Authorization Tool
MEDIUM	2406783	BC-INS-CTC	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Central Technical Configuration
MEDIUM	2426076	FIN-SEM-SRM	Multiple vulnerabilities in SAP ERP Stakeholder Relationship Management
MEDIUM	2400292	BC-DWB-JAV-CAF	Missing XML Validation vulnerability in TranslationSupport application
MEDIUM	2387249	EP-KM-CM-ICE	Missing XML Validation vulnerability in Knowledge Management ICE Service
MEDIUM	2308535	BC-ILM-DAS	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Java Archiving Framework
MEDIUM	2417355	BC-MID-RFC	Missing Authorization check in RFC Destination Maintenance
MEDIUM	2446435	FS-QUO	Information Disclosure in FS-QUO
MEDIUM	2452697	FS-BA-RD	Missing Authorization check in RDL

Appendix: SAP Security Notes, April 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2433458	BC-DWB-TOO-DBG	Missing Authorization check in ABAP Debugger
LOW	2403010	BI-BIP-INV	Cross-Site Request Forgery (CSRF) vulnerability in BI LaunchPad

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

© Copyright Layer Seven Security 2017 - 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.