LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

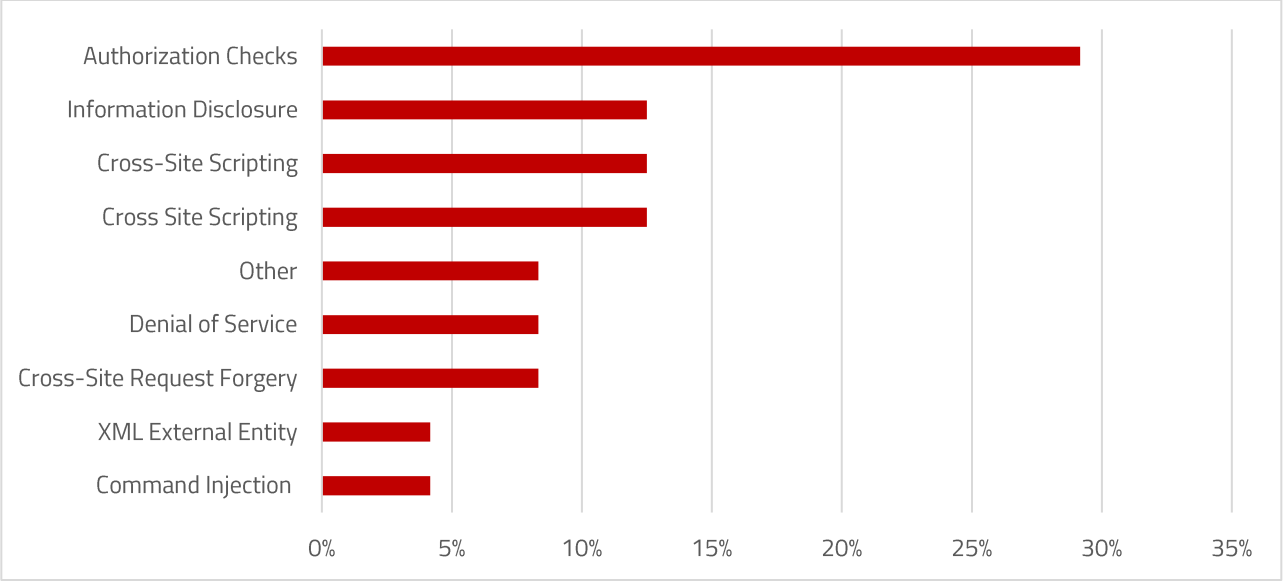
January 2019

SAP Security Notes

January 2019

Hot News Note 2696233 deals with multiple vulnerabilities in the SAP Cloud Connector. The Connector is an agent that connects on premise systems with applications operating on the SAP Cloud Platform. The agent supports HTTP, RFC, JDBC/ODBC and other connections between on-premise and cloud installations using reverse invoke without requiring inbound ports to be opened in on-premise network firewalls. Therefore, the Connector is designed to support secure cloud and on-premise connectivity. Note 2696233 patches a missing authentication vulnerability in the SAP Cloud Connector with a CVSS score of 9.3/10. It also addresses a lower-risk code injection vulnerability that could lead to information disclosure or a denial of service in the Connector. Customers are advised to upgrade to SAP Cloud Connector 2.11.3 to remove the vulnerabilities.

Hot News Note 2727624 includes corrections for removing a critical information disclosure vulnerability in SAP Landscape Management. Landscape Management supports system cloning, copying, refreshing and other system administration tasks. The vulnerability addressed by Note 2727624 could be exploited by attackers to steal user credentials. The note recommends deleting entries in log files and changing passwords for system users that may be disclosed in logs.



SAP Security Notes by Vulnerability Type

Other high priority notes include 2727623 which removes a missing authorization check in SAP BW/4HANA and Note 2724788 which tackles various vulnerabilities in the Adobe PDF Print Library.

Appendix: SAP Security Notes, January 2019

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for the browser control Chromium delivered with SAP Business Client
HOT NEWS	2727624	BC-VCM-LVM	[CVE-2019-0249] Information Disclosure in SAP Landscape Management
HOT NEWS	2696233	BC-MID-SCC	[CVE-2019-0246] Multiple Vulnerabilities in SAP Cloud Connector
HIGH	2727623	BW4-DM-MD	[CVE-2019-0243] Missing Authorization check in SAP BW/4HANA
HIGH	2724788	XX-PART-ADB-PRN	Various Vulnerabilities in ADOBE PDFPRINT LIBRARY
MEDIUM	2425129	BC-UPG-NA	Missing XML Validation vulnerability in SAP Note Assistant
MEDIUM	2719415	FI-LOC-SRF-RUN	Cross-Site Request Forgery (CSRF) vulnerability in SAP S/4 HANA for Advanced Compliance Reporting/ Run Advanced Compliance Report
MEDIUM	2429274	IS-B-BCA	Switchable Authorization checks in SAP Enterprise Financial Services
MEDIUM	2473860	FIN-FSCM-TRM-TM	Authorization check for RFC in SAP Finance Transaction Manager
MEDIUM	2705945	FI-LOC-SRF-RUN	Cross-Site Request Forgery (CSRF) vulnerability in SAP S/4 HANA for Advanced Compliance Reporting/ Run Advanced Compliance Report
MEDIUM	2574897	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2602928	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in Text Editors for SAP CRM WebClient UI
MEDIUM	2601676	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2725538	MOB-SDK-AGC	[CVE-2019-0241] Denial of service (DOS) in SAP Work and Inventory Manager
MEDIUM	2724059	MOB-APP-BI-AND	[CVE-2019-0240] Denial of service (DOS) in SAP Business Objects Mobile for Android
MEDIUM	2723142	OPU-GW-COR	[CVE-2019-0248] Information Disclosure in SAP Gateway of ABAP Application Server
MEDIUM	2607692	CA-WUI-UI	[CVE-2019-0245] Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2699233	EPM-EA-DEP	[CVE-2018-2499] Information Disclosure in SAP Financial Consolidation Cube Designer

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2697573	CEC-COM-CPS-WEB	[CVE-2019-0238] Cross-Site Scripting (XSS) vulnerability in SAP Commerce (ex. SAP Hybris Commerce)
MEDIUM	2690274	FI-CF-INF	Switchable Authorization checks for RFC in SAP Central Finance - Data Flow Verification
MEDIUM	2662687	IS-B-BCA-MD	[CVE-2018-2484] Missing Authorization check in SAP Enterprise Financial Services
MEDIUM	2490047	LO-MD-BP-CM	Switchable Authorization checks for RFC in Customer Master Data
MEDIUM	2588763	CA-WUI-UI-TAG	[CVE-2019-0244] Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2495144	FI-CF-INF	Switchable Authorization checks for RFC in Central Finance

LAYER SEVEN SECURITY

Layer Seven Security secure, patch and monitor SAP systems against cyber threats using SAP Solution Manager. Layer Seven's innovative and patent-pending Cybersecurity Extension for Solution Manager extends the capabilities of Solution Manager for advanced vulnerability management, threat detection and incident response.

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 2019 - 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.