




LAYER SEVEN SECURITY

SAP Security Notes

April 2018

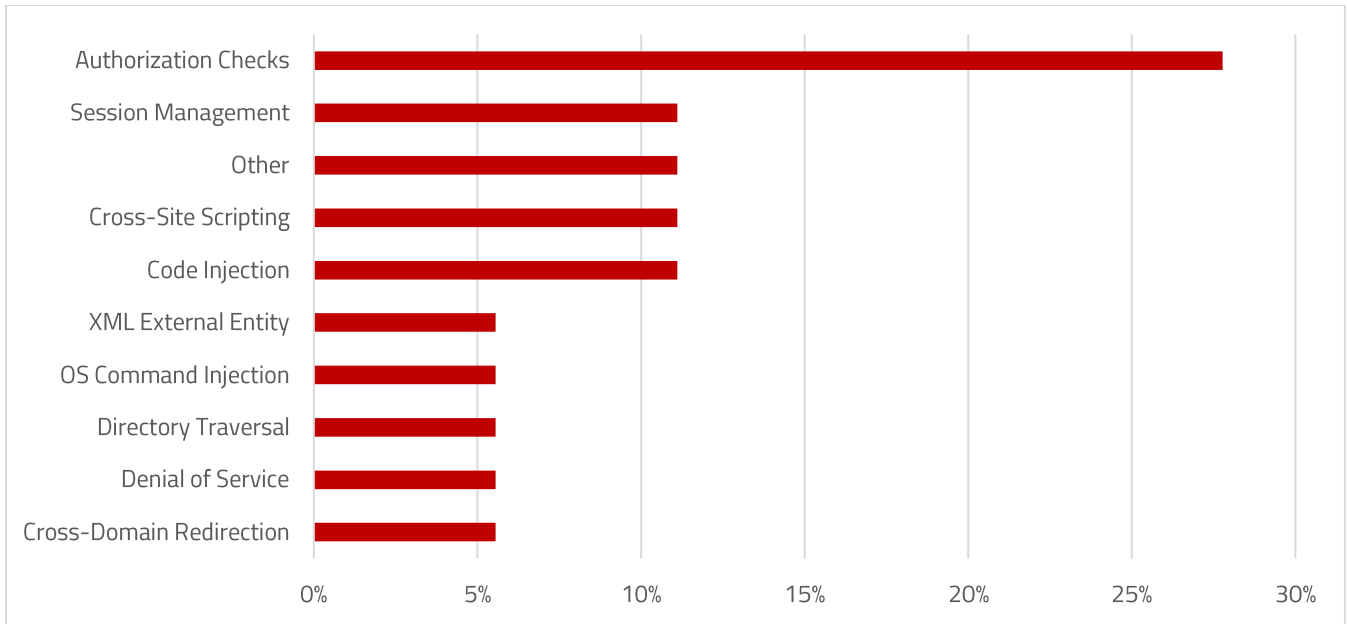


Hot News Note 2622660 includes critical security updates for web browser controls delivered with SAP Business Client. The Client provides a unified environment for SAP applications including Fiori, SAP GUI, and Web Dynpro. It supports browser controls from Internet Explorer (IE) and Chrome for displaying HTML content. Security corrections for the WebBrowser control of the .NET framework in IE are delivered directly by Microsoft. Unlike IE, the browser control for Chrome is embedded in SAP Business Client using the open source Chromium Embedded Framework (CEF). Security fixes are provided by the Chromium project and delivered by SAP through periodic Security Notes. Note 2622660 includes corrections addressed by Chromium releases 64 and 65. The critical rating of the note is due to the fact that the highest CVSS rating of the security corrections bundled in the fixes is 9.8/10.

Note 2552318 provides an important update for Note 2376081 released in August 2017. The note deals with a high priority code injection vulnerability impacting iviews created in Visual Composer. Iviews are interactive, web-based applications in Java platforms. The corrections included in Notes 2552318 and 2376081 will support code injection checks for the entire input stream received from Visual Composer in the export to Excel mechanism. Note 2376081 should be implemented before 2552318.

SAP Security Notes

April 2018



SAP Security Notes by Vulnerability Type

Note 2537150 includes corrections to automatically terminate active sessions for users whose passwords have been changed in BusinessObjects.

Note 2587985 provides instructions for removing a Denial of Service (DOS) vulnerability the in the Apache Http Server embedded in SAP Business One.

Finally, Note 2190621 provides a solution to log peer IP addresses instead of terminal IP addresses in the Security Audit Log. Peer or routed IP addresses are less vulnerable to manipulation than terminal IP addresses.

Appendix: SAP Security Notes, April 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for web browser controls delivered with SAP Business Client
HIGH	2376081	EP-VC-04S	Code Injection vulnerability in Visual Composer 04s iviews
HIGH	2552318	EP-VC-04S	Update 1 to Security Note 2376081
HIGH	2537150	BI-BIP-INV	[CVE-2018-2408] Improper Session Management in SAP Business Objects - CMC/BI Launchpad/Fiorified BI Launchpad
HIGH	2587985	SBO-CRO-SEC	Denial of Service (DOS) in SAP Business One
MEDIUM	2187594	EHS-MGM-FND	Code injection vulnerability in EHS-MGM-FND
MEDIUM	2081029	BC-WD-ABA	Potentially false redirection of Web site content in Web Dynpro ABAP application
MEDIUM	2190621	BC-CST-GW	SAP Netweaver SAL incorrect logging of addresses
MEDIUM	2497027	XX-CSC-BR-NFE	Missing Authorization check in XX-CSC-BR-NFE
MEDIUM	2497000	XX-CSC-BR-NFEIN	Missing Authorization check in XX-CSC-BR-NFEIN
MEDIUM	2372688	SV-SMG-SUP	[CVE-2018-2405] Cross-Site Scripting in Solution Manager Incident Management Workcenter
MEDIUM	2560132	BI-RA-CR	[CVE-2018-2406] Unquoted windows search path vulnerability in Crystal Reports Server, OEM Edition
MEDIUM	2582870	SBO-CRO-SEC	[CVE-2018-2410] Cross-Site Scripting (XSS) Vulnerability in SAP Business One Browser Access
MEDIUM	2614141	BC-MID-SCC	[CVE-2018-2409] Improper session management when using SAP CP Connectivity Service and Cloud Connector
MEDIUM	2598687	BC-SYB-ASE	Missing XML Validation vulnerability in SAP Control Center and SAP Cockpit Framework
MEDIUM	2595800	EPM-DSM-GEN	[CVE-2018-2403] Multiple Security Vulnerabilities in SAP Disclosure Management
MEDIUM	2473452	FS-CMS-MD	Missing Authorization check in FS-CMS
LOW	2608312	FI-CF-INF	Switchable Authorization checks in Central Finance



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 2018 - 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.