Layer Seven Security

ADVISORY

SAP Security Notes

February 2016

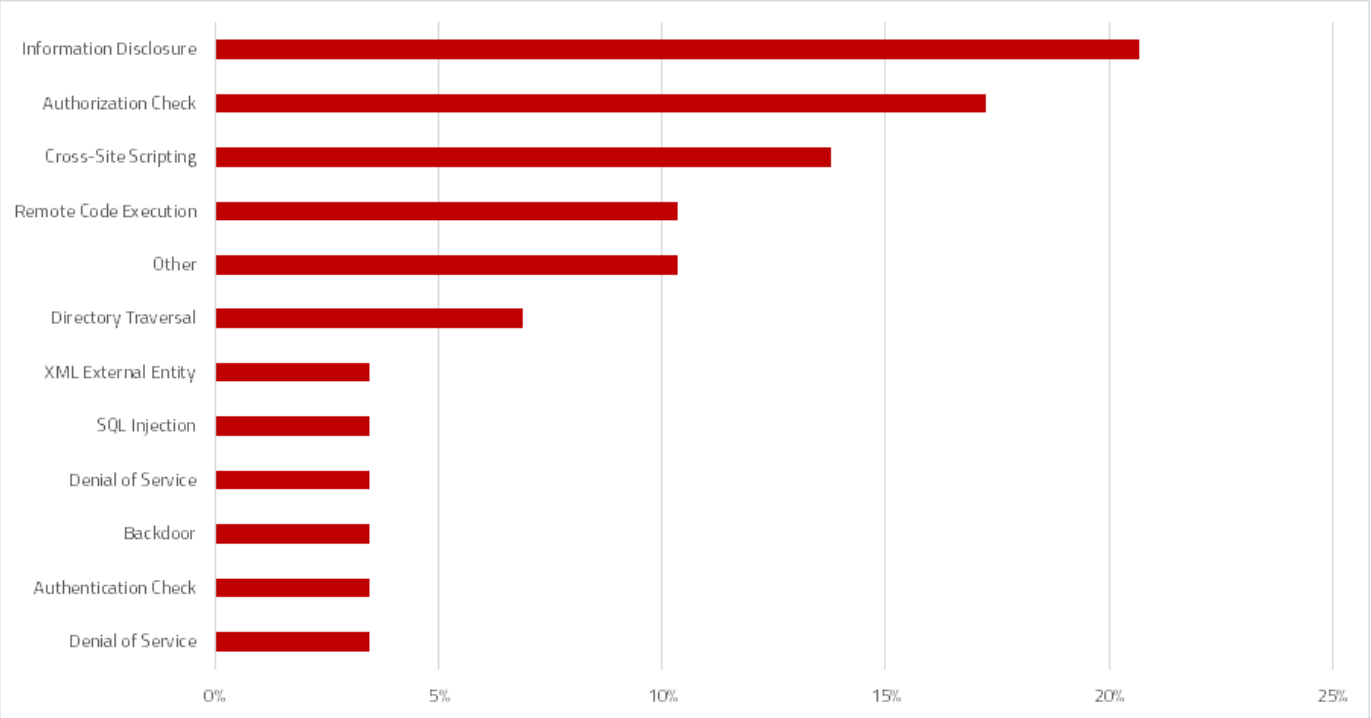
SAP Security Notes

February 2016

SAP released a Hot News patch for version 8.0 of the Visual Enterprise suite in February. This includes the Author, Generator and Viewer applications used to create and manage 3D data visualizations. Note 2281195 addresses a memory corruption vulnerability that can be exploited to perform a denial of service through .skp files read by Visual Enterprise. The specific memory corruption error addressed by the Note appears to be a buffer overflow flaw. This can lead to a denial of service if a system terminates an application process when the application attempts to read memory outside it's allocated space. Customers should upgrade to versions 8.0 SP04 MP3 and enable the sandboxing option for Visual Enterprise applications.

In addition to the Notes released in January, SAP released several more Notes in February for products impacted by the Java deserialization vulnerability in open-source Apache libraries such as the Commons Collections. This includes Note 2262104 for Wily Introscope Manager, Note 2246851 for Process Integration, and Note 2268810 for SAP Lumira. All three Notes are rated as high priority given the severity of the threat posed by the Java deserialization vulnerability.

Note 2273831 provides a patch to prevent attackers from executing remote commands on TREX / BWA hosts using the privileges of the <SID>ADM user. The Note supplements Note 2234226 which recommends isolating TREX/ BWA systems from other systems using a separate subnet. Since using separate subnets is not possible in all scenarios, Note 2273831 introduces an access control to



SAP Security Notes by Vulnerability Type

prevent processes operating on remote systems from accessing the internal TREX/ BWA interface.

Note 2252312 delivers an important change to ensure events related to RFC callbacks are logged by the Security Audit Log with the appropriate severity rating. This will ensure such events are captured by filters that are configured to record only critical events within each client.

Finally, Note 2245130 provides a kernel patch and correction instructions to remove a potential bypass of runtime checks performed by Unified Connectivity (UCON) to control external access to remote-enabled function modules. The Note applies to versions 7.40 and higher of the software component SAP_BASIS.

Appendix: SAP Security Notes, February 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2281195	CA-VE-VEV	Potential remote termination of running processes in SAP Visual Enterprise Author, Generator and Viewer
HIGH	2037304	SV-SMG-SDD	Lacks proper input validation in SDCC Download Function Module
HIGH	2273881	BC-TRX	Update 1 to Security Note 2234226
HIGH	2249364	BC-CTS-SDIC	Unauthorized modification of displayed content in SDIC
HIGH	2256846	EP-BC-UWL	Potential information disclosure relating to usernames
HIGH	2262104	XX-PART-WILY	Security vulnerabilities found in Apache Commons Collections library used in CA Introscope
HIGH	2272211	HAN-AS-XS	Update of SAPUI5 version in SAP HANA due to security note 2204160
HIGH	2220571	BC-XI-CON-JPR	Unauthorized modification of displayed content in Java Proxy Runtime
HIGH	2228405	EP-PIN-CS	Unauthorized modification of stored content in EPCF Loader Tester
HIGH	2230978	MFG-MII	Directory traversal in MFG-MII
HIGH	2234226	BC-TRX	TREX / BWA: Potential technical information disclosure / host OS compromise
HIGH	2235088	BC-JAS-WEB	Directory traversal in JSF
HIGH	2101079	BC-ESI-UDDI	Potential modif./disclosure of persisted data in BC-ESI-UDDI
HIGH	2246851	BC-XI-IBD	PI SEC: Security vulnerabilities found in Apache Commons Collections library used in Enterprise Services Repository
HIGH	2268810	BI-LUM-DSK	Security vulnerability in Apache Commons Collections library used by multiple SAP Lumira products
MEDIUM	2064501	BW-WHM-DBA	Missing authorization check in BW-WHM-DBA
MEDIUM	2069820	BW-BEX-ET	Missing authorization check in BW-BEX-ET
MEDIUM	2069994	BW-SYS-DB	Potential information disclosure relating to user email
MEDIUM	1905286	MDM-GDS	Hard-coded credentials in MDM-GDS
MEDIUM	1771200	BC-JAS-COR	Potential information disclosure relating to AS Java
MEDIUM	1658568	BC-JAS-SEC-LGN	Missing access restrictions
MEDIUM	2085214	XAP-EM	Untrusted XML input parsing possible in SAP Environmental Compliance 3.0
MEDIUM	2252312	BC-MID-RFC	Insufficient logging of RFC in SAL
MEDIUM	2258608	BC-ABA	Missing Authentication in Transaction DBCO
MEDIUM	2236289	BC-DB-MSS	Missing authorization check in SMSS_GET_DBCON
MEDIUM	2245130	BC-MID-RFC	Potential bypass of unified connectivity runtime checks possible in BC-MID-RFC
MEDIUM	2266565	BC-SEC	SAPSSOEXT process crash during ticket verification
MEDIUM	2177403	IS-A-VMS	Missing authorization check in IS-A-VMS
LOW	2196420	BW-BEX-ET-WB-7X	Potential information disclosure relating to BW-BEX-ET-WB-7X

LAYER SEVEN SECURITY

Layer Seven Security empowers organisations to realize the potential of SAP systems. We serve customers worldwide to secure systems from cyber threats. We take an integrated approach to build layered controls for defense in depth

Address
Westbury Corporate Centre
Suite 101
2275 Upper Middle Road
Oakville, Ontario
L6H 0C3, Canada

Web
www.layersevensecurity.com
Email
info@layersevensecurity.com
Telephone
1 888 995 0993

© Copyright Layer Seven Security 2016 - 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.