Layer Seven Security

ADVISORY

SAP Security Notes

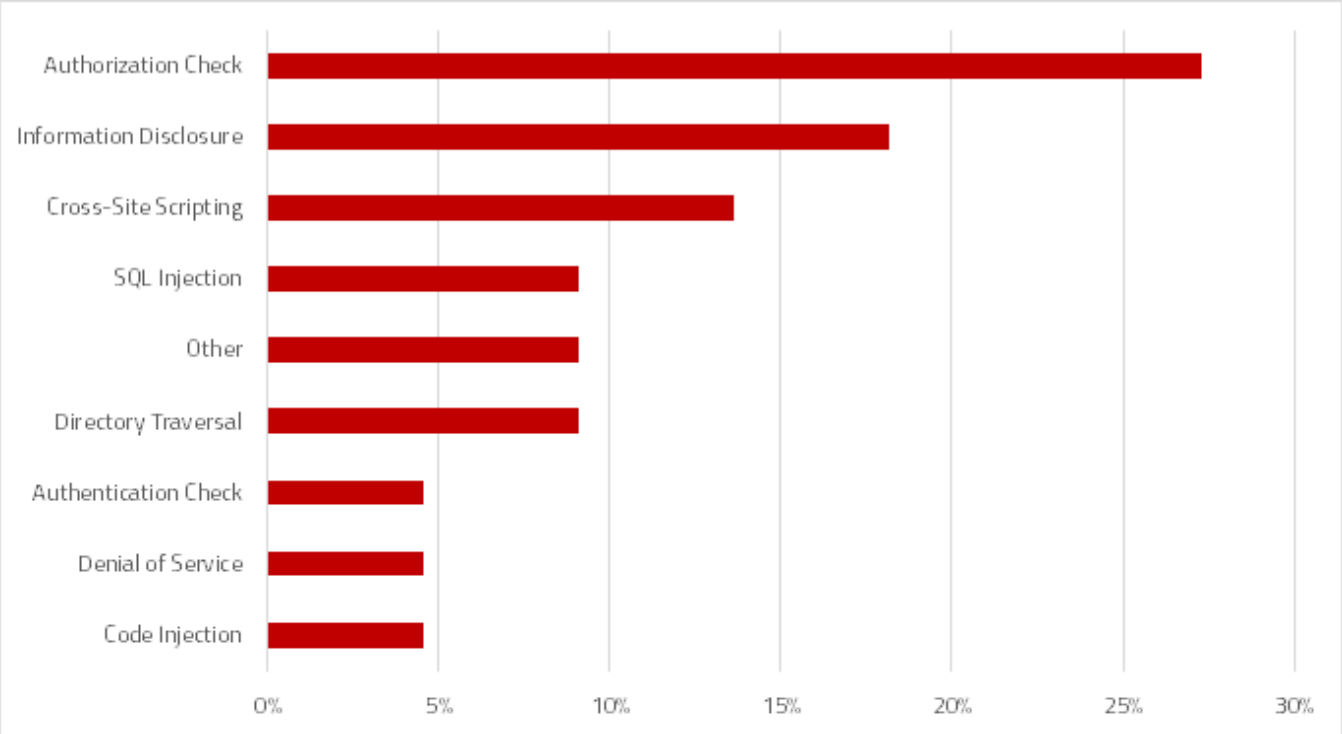
July 2015

SAP Security Notes

July 2015

The most significant Security Note released by SAP in July deals with a critical missing authentication and authorization check in the XP Server of the Sybase ASE database platform. The XP Server is an Open Server application that runs on the same host as ASE. It executes extended stored procedures and communicates with ASE through remote procedure calls (RPC). Prior to the release of Note 2180049 in July, no special permissions were required to run the XP Server. Therefore, unauthenticated users could exploit the Server to perform arbitrary OS commands against the host. This could provide attackers with complete control over the host and ASE. The severity of the risk supports the high CVSS rating of 9.3/10 provided by SAP for Note 2180049. Customers are strongly advised to upgrade ASE to the latest SP level to address the risk. Customers that are not using extended stored procedures can elect to disable the XP Server by following the instructions provided in the Note. The Server is started automatically during the ASE start-up procedure.

Note 2141629 patches a high risk information disclosure vulnerability that could be exploited to leak usernames and passwords from the System Landscape Directory (SLD) of systems running NetWeaver AS Java. The SLD uses the Common Information Model for the centralized storage and maintenance of data for technical or logical systems. The SLD can include not only Java systems, but ABAP and other platforms and standalone components such as the SAP start service. Notes 1985340 and 2189127 address a similar vulnerability in administrative components of AS Java.



SAP Security Notes by Vulnerability Type

Note 1971294 addresses a vulnerability in the Query Builder Application of BusinessObjects that could lead attackers to obtain the authentication information of users. The vulnerability arises when the secure flag is not set on cookies required by the application. The Query Builder is used to query data in tables within the BusinessObjects repository.

Approximately 1 on 4 of July's Security Notes are intended to correct authorization issues including vulnerabilities that could lead to an escalation of privileges. The most important include Notes 2147415, 1611408 and 2166077 impacting critical SAP applications and components such as CRM, Sales and Distribution and the ABAP Workbench. These areas impact sensitive areas such as sales processes and procedures, material information, and tools used to create, edit and activate ABAP programs.

Appendix: SAP Security Notes, July 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2180049	BC-SYB-ASE	Missing authentication check in SAP ASE XPServer
HIGH	2113721	BI-BIP-LCM	Unauthorized modification of displayed content in BI-BIP-LCM
HIGH	1952092	XX-IDES	Code injection vulnerability in IDES systems
HIGH	2141629	BC-CCM-SLD	Potential information disclosure relating to NW AS Java
HIGH	1971294	BI-BIP-ADM	Secure' flag was not set on cookies for Query Builder Application
HIGH	2147415	CRM-BTX-ANA	Missing authorization check in CRM-BTX-ANA.
HIGH	2170931	BC-DWB-TOO-SFW	Missing authorization check in SAP Switch Framework
HIGH	2166077	BC-DWB-TOO-ABA	Missing authorization check in ABAP Workbench
HIGH	1611408	SD-SLS	Missing authorization check in SD-SLS
HIGH	1985340	BC-JAS-ADM-ADM	Potential information disclosure relating to NW AS Java
HIGH	2189127	BC-JAS-ADM-ADM	Update 1 to Security Note 1985340
MEDIUM	2182488	CA-EPC	Open source vulnerabilities Axis 1.x in SAP EPC 2.0
MEDIUM	2079002	BC-JAS-SEC-LGN	Unauthorized modification of displayed content in logon application
MEDIUM	1955742	BC-JAS-SEC-LGN	Potential Denial of Service in SAML2
MEDIUM	1791940	IS-DFS-MA	Potential modification of persisted data in MDS
MEDIUM	1945215	BC-ILM-DAS	Missing authorization check in XML Data Archiving Service
MEDIUM	1922205	BC-XI-IS-WKB	Authorization default value in component BC-XI-IS-WKB
MEDIUM	2149517	BC-JAS-ADM-ADM	Unauthorized modification of displayed content in NetWeaver Administrator
MEDIUM	2148854	HAN-AS-XS	Potential information disclosure relating to server information
MEDIUM	1861588	XX-CSC-PT-FIAA	Directory traversal in XX-CSC-PT-FIAA
MEDIUM	2157355	XX-CSC-RO-FI	Potential disclosure of persisted data in include /CEECV/ ROLO_RMIMSELS
MEDIUM	2156556	XX-CSC-GR-FI	Directory traversal in module pool SAPMJ1GFBWE

LAYER SEVEN SECURITY

Layer Seven Security empowers organizations 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 2015 - 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.