ADVISORY

Layer Seven Security

SAP Security Notes

January 2013

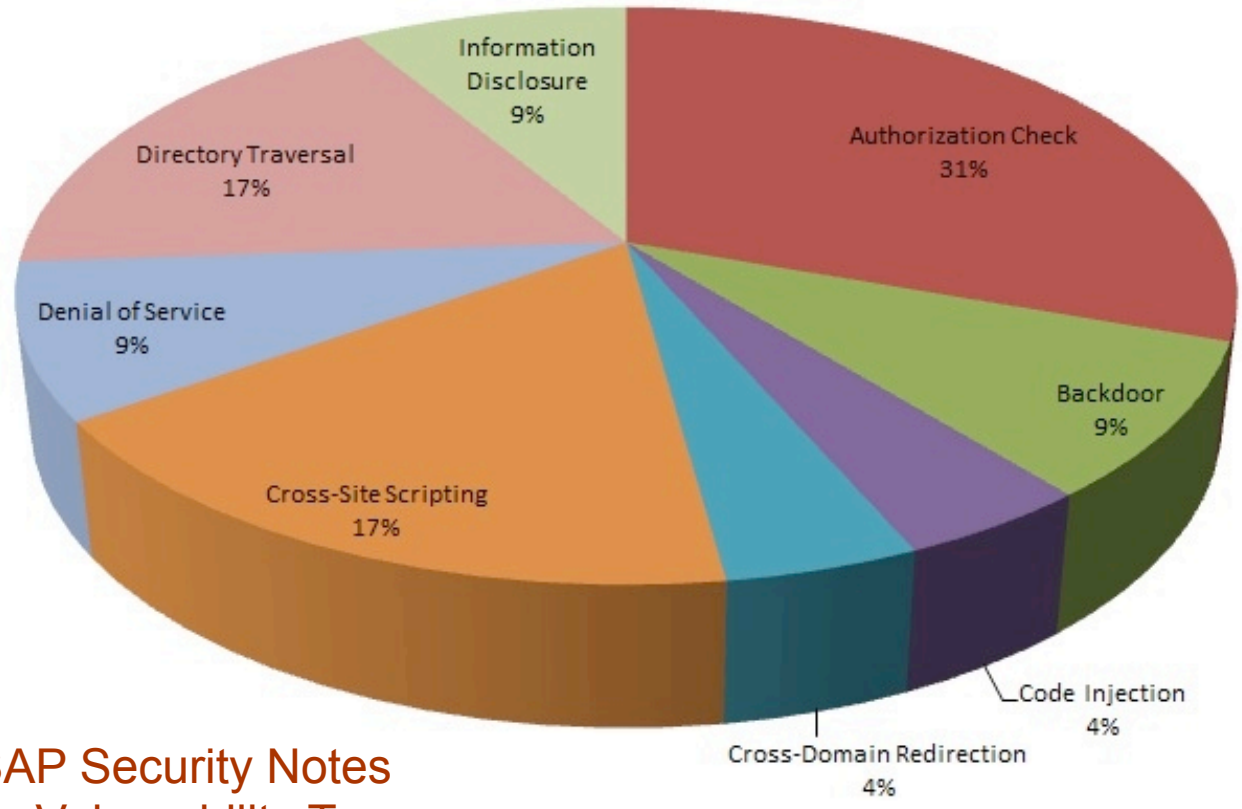
SAP Security Notes

January 2013

There were several Security Notes released by SAP in January for directory traversal vulnerabilities affecting a number of application areas. The most important affected the adminadapter service in the Java Application Server used for system administration and monitoring (Note 1755108). The vulnerability patched by the Note carried a CVSS Base Score of 10.0. Scores range between 1-10. Critical vulnerabilities are generally rated between 7.5 - 10.0. Other areas patched for directory traversal risks include Material Planning Objects (MPO) used for equipment and armament management by organizations using the SAP industry solution Defense Forces and Public Security (IS-DFS) (Note 1787460) and the Integration Builder Framework of Process Integration (PI), formerly known as Exchange Infrastructure (XI) (Note 1628537).

Directory traversal, also known as path traversal, occurs when an attacker is able to successfully access directories or files outside of restricted zones by modifying the external input processed by application servers. This can provide access to parent directories (relative path traversal) or any directory on a server (absolute path traversal). The consequences of directory traversal can be severe, ranging from viewing data in sensitive password, program or other files in directories, to corrupting or removing the files which can lead to Denial of Service (DoS). It can be prevented through secure coding that includes requirements for the validation of inputs against a whitelist of acceptable values for properties such as length, type, syntax and file extensions. For more information, refer to the Common Weaknesses Enumeration (CWE), sponsored by the Office of Cybersecurity and Communications at the Department of Homeland Security.

SAP also released several Notes for missing authorization checks. This includes the U.S version of Personnel Administration (PA-PA-US) which prior to the release of Note



SAP Security Notes by Vulnerability Type

1779317 did not perform sufficient authorization checks for access to HR Distributed Reporting. It also includes ABAP Web Services, a Basis component in the Enterprise Service Infrastructure (Note 1776984).

Other noteworthy Security Notes include 1731362 which patches a buffer overflow vulnerability in the Communications Management Software of CRM, and 1674132 which deals with a code injection flaw when using the File Transfer Protocol (FTP) in SAPconnect during external communications.

SAP customers should also review Notes 1775422 and 1772208. Both provide corrections for hardcoded username and password combinations contained in program codes that enable attackers to access system resources without authorization or enable legitimate users to escalate their privileges. The affected programs are the Business Navigator component of Customizing (IMG) and the Basis Application Log.

Appendix: SAP Security Notes, January 2013

PRIORITY	NOTE	AREA	DESCRIPTION
1	1755108	BC-JAS-ADM-ADM	Directory traversal in adminadapter service
2	1724922	BC-WD-JAV	Update 1 to Security Note 1653474
2	1787460	IS-DFS-OF-MPO	Directory-Traversal in IS-DFS-OF-MPO
2	1785747	BW-BEX-OT	Missing authorization check in BW-BEX-OT
2	1784654	BW-BEX-ET	Missing authorization check in BW-BEX-ET
2	1779317	PA-PA-US	Missing authorization check in HR Distributed-Reporting - CE
2	1776984	BC-ESI-WS-ABA	Missing authorization check in component SAP_BASIS
2	1775527	BC-SRV-COM-FTP	Update 1 to Security Note 1692988
2	1775422	BC-CUS-TOL-NAV	Hard-coded credentials in BC-CUS-TOL-NAV
2	1731362	CRM-BCM	Potential remote code execution in SAP BCM SIP
2	1674132	BC-SRV-COM-FTP	Code injection vulnerability in BC-SRV-COM-FTP
2	1673016	EHS-DGP-TP	Missing authorization check when branching to phrase mgmt
2	1628537	BC-XI-IBF	Directory Traversal in Exportability Check Servlet
3	1784770	BI-RA-CR	Unauthorized modification of displayed content in CR Server
3	1794299	XX-PROJ-FI-CA	Potential information disclosure relating to FI-CA
3	1772208	BC-SRV-BAL	Hard-coded credentials in BC-SRV-BAL
3	1765267	BC-ESI-UDDI	Unauthorized modification of displayed content in ESREGBASIC
3	1761018	BC-COM-WIK	Unauthorized modification of stored content in BC-COM-WIK
3	1748669	BC-SRV-KPR-CS	Potential information disclosure relating to ContentServer
3	1729293	BC-CCM-MON	Untrusted XML input parsing possible in GRMG
3	1725390	BC-CCM-MON	Untrusted XML input parsing possible in GRMG
3	1597256	SCM-APO-FCS-MAP	Missing authorization check in SCM-APO-FCS-MAP
3	1412864	BW-BEX-ET-XC	Redirection of Web site in Xcelsius may be incorrect

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 2013 - 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.