Layer Seven Security

ADVISORY

SAP Security Notes

February 2013

SAP Security Notes

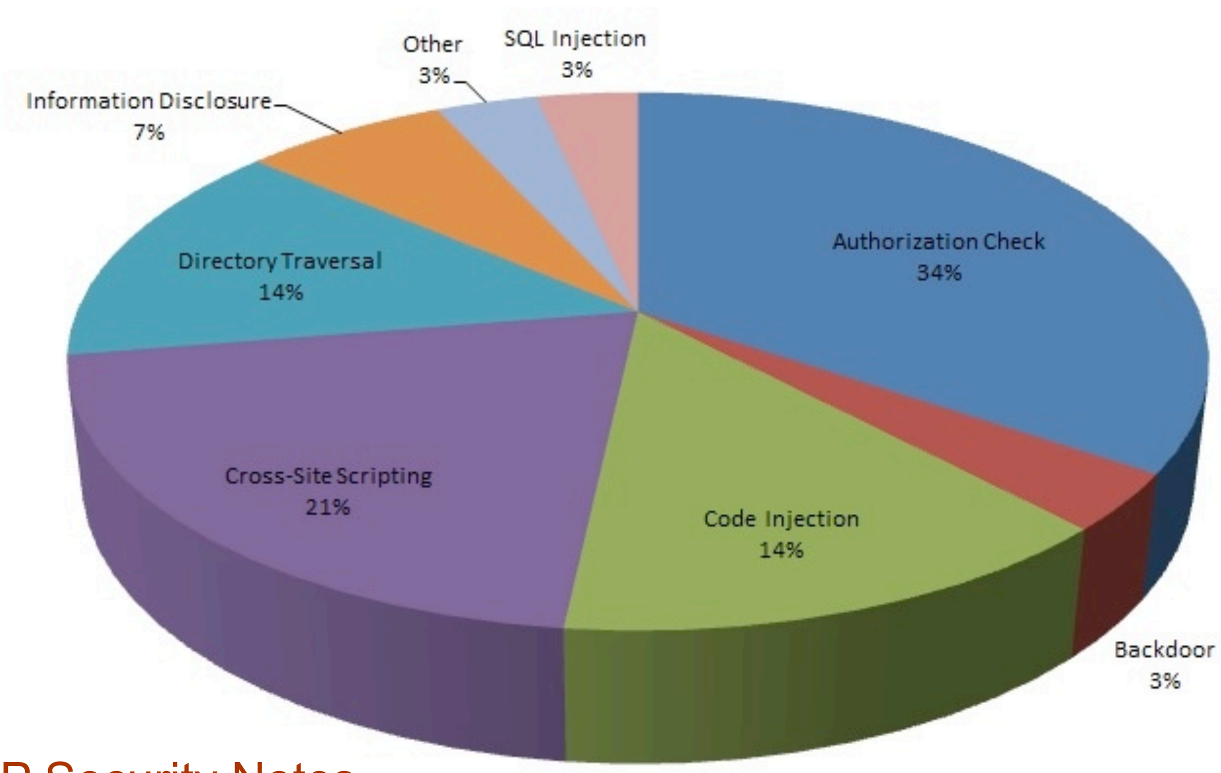
February 2013

SAP Security Notes are rarely front page news. The exception was Note 1785761 which was singled out by SAP for a call to action in the Spotlight News section of the Support Portal after February's Patch Day. The decision was warranted given the high CVSS score of the issue reported by the Note and the fact that it related to an escalation of privileges vulnerability in RFC components of the NetWeaver Application Server. RFC is SAP’s main communication protocol and is used to integrate system environments and landscapes. Customers operating NetWeaver releases 7.00 and 7.01 in combination with the 7.20 or 7.21 downward compatible kernel are strongly advised to update the patch level of the SAP kernel.

Curiously, SAP made no mention in the call to action of the other crucial Security Note released in February, despite the fact that it carried the highest possible CVSS score of 10.0. Note 1800603 released a patch for a buffer overflow vulnerability in the Message Server, used for load balancing and managing communications between application servers in SAP systems. The vulnerability could be exploited to take control of the Message Server through the injection of malicious code in the working memory of the component.

A code injection vulnerability in the Test Data Migration Server (DMIS_CNT) component of CA-EUR was also patched in February. CA-EUR is designed to facilitate the change-over from local currencies to the Euro. The vulnerability addressed by Note 1788426 could be exploited to obtain sensitive information, modify or delete data, create privileged users or perform a denial of service attack.

Note 1796264 contended with similar vulnerabilities in Directory Services (BC-SEC-DIR) and programs used to detect and report issues with the Virus Scan Interface (BC-SEC-VIR).



SAP Security Notes by Vulnerability Type

Both are important components of the Basis security module. Directory Services is used to store access-related information in a central location for multiple, connected systems. This includes user names, departments, organizations and authorizations, public key certificates and system IDs.

An SMBRelay vulnerability in the SAP List Viewer was patched through Note 1446476. The List Viewer uses grid control to standardize the presentation of columns in lists containing data fields. SMBRelay uses the NetBIOS port 139 to execute Man-in-the-Middle and other attacks against Windows systems. Port 139 is often opened for file and printer sharing in Windows, despite known security issues.

Finally, SAP GRC 5.3 was subject to several security patches for vulnerabilities including backdoors, cross-site scripting, directory traversal, and SQL injection that could enable attackers to modify application content and obtain authentication information from legitimate users. The specific areas affected by these vulnerabilities include VIRSA components within ARA, ARQ and BRM. Customers should implement Support Pack 20 to close the vulnerabilities.

Appendix: SAP Security Notes, February 2013

PRIORITY	NOTE	AREA	DESCRIPTION
1	1785761	BC-MID-RFC	Missing authorization check in RFC
1	1800603	BC-CST-MS	Potential remote code execution in Message Server
2	1777228	CO-PC-PCP	Missing authorization check in CO-PC-PCP
2	1785690	EP-PIN-RTM	unauthorized access using RTMF
2	1788426	CA-EUR	Code injection vulnerability in CA-EUR (DMIS_CNT)
2	1788614	SV-SMG-SDD	Missing authorization check in ST-PI
2	1791089	CA-EUR	Missing authorization check in DMIS
2	1792354	CA-EUR	Missing authorization check in DMIS_EXT
2	1795948	CA-EUR	Missing authorization check in CDOP
2	1796264	BC-SEC-DIR	Code injection vulnerability in LDAP- and VSCAN-Customizing
2	1750997	BC-FES-CTL	Missing authorization check in BC-FES-CTL
2	1757675	BC-CTS-CMS	Directory traversal in DI_CMS, LM-TOOLS, LM-CTS, SAP_DEVINF
2	1767955	BC-SRV-KPR-CS	Unauthorized modification of stored content in BC-SRV-KPR-CS
2	1767956	BC-SRV-KPR-CS	Directory traversal in BC-SRV-KPR-CS
2	1818523	CRM-BF-ML	Update #1 to Security Note 1660855
3	1819543	BC-SRV-COM-FTP	Update 1 to security note 1391655
3	1770722	BC-FES-GUI	Potential logon information disclosure in SAP GUI
3	1771201	BC-FES-GUI	Potential logon information disclosure in SAP Portal&amp;WinGUI
3	1790440	FIN-FSCM-TRM-TM	Missing authorization check in Component Transaction Manager
3	1446476	BC-SRV-ALV	SMBRelay in SAP ALV
3	1700532	CA-GTF-RCM	Unauthorized modification of displayed content in CA-GTF-RCM
3	1743637	WEC-FRW-JSF	Directory traversal in Web Channel Experience Management
3	1763218	GRC-SAC-BRM	Unauthorized modification of stored content in GRC AC 5.3
3	1763222	GRC-SAC-BRM	Directory traversal in GRC AC 5.3
3	1763695	GRC-SAC-ARQ	Unauthorized modification of displayed content in GRC 5.3
3	1763796	GRC-SAC-ARQ	Hard-coded credentials in GRC 5.3
3	1763797	GRC-SAC-ARQ	Cross-Site-Scripting (XSS) in GRC 5.3
3	1763798	GRC-SAC-ARQ	Potential modif./disclosure of persisted data in GRC 5.3
3	1764994	BC-DB-SDB	Potential remote code execution via dbmcli

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

SAP Partner

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.