Layer Seven Security

ADVISORY

SAP Security Notes

September 2014

SAP Security Notes

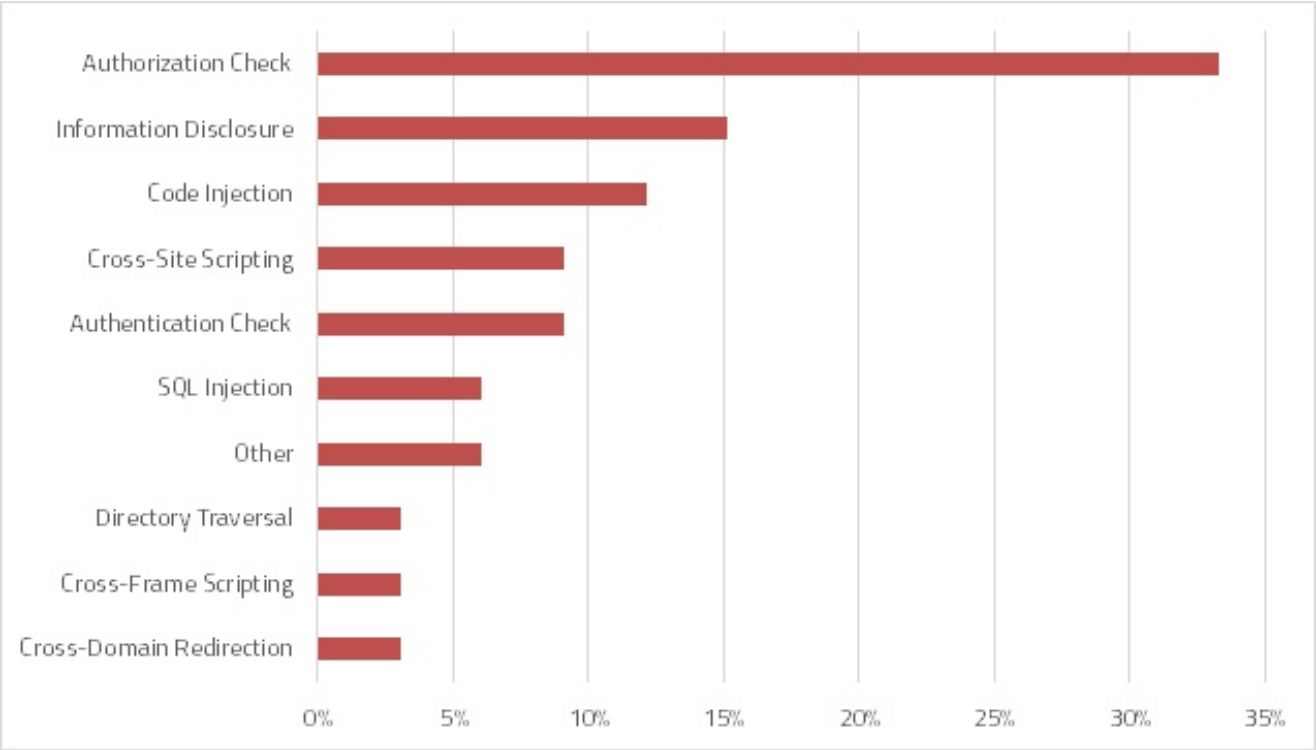
September 2014

September's corrections included a number of patches for missing authorization checks in critical applications and components, most notably areas such as SD-BIL-IV, used for payment card processing in Sales & Distribution (Note 2035923), Claims Management in Financial Services (Note 2042338), and the Batch Input Recorder (Note 1979454). Corrections for the latter are largely manual and must be implemented separately in each system.

Note 2043506 resolved a high risk priority vulnerability in the File System Browser of Solution Manager. The Browser is used by applications such as Root Cause Analysis to read operating system files in managed systems through Diagnostics Agents. The Note introduces a Java aglet with a white list property that can be used to control file extensions accessed through the File System Browser. The white list can be edited with the SAP_RCA_AGT_ADM role.

Note 1984050 patched a vulnerability in SAP Business One Cloud that could enable attackers to eavesdrop on communication traffic between clients and servers and access authentication and other information in data transmissions. Business One Cloud provides cloud-based functionality for critical services such as accounting and finance, sales and customer management, purchasing and operations, and inventory and distribution.

Note 2028904 introduced protection for browsers vulnerable to cross-frame scripting (XFS). XSF attacks commonly exploit cross-site scripting vulnerabilities to inject frames containing malicious javascript designed to capture sensitive data keyed into web pages. There are known vulnerabilities in the security models of browsers that should prevent the sharing of data between windows or frames loaded from different origin servers or domains. These vulnerabilities could lead to the theft of information such as logon credentials.



SAP Security Notes by Vulnerability Type

The corrections delivered in Note 2028904 apply to the logon application of the Internet Communication Framework (ICF). This is an ABAP interface for HTTP, HTTPS and SMTP. The ICF receives Web-based calls through the Internet Communication Manager (ICM).

Note 2049371 patches an OpenSSL vulnerability in Sybase products that could be exploited to perform a man-in-the-middle attack to decrypt and modify traffic between clients and servers. The vulnerability effects all clients but only servers using OpenSSL versions 1.0.1 and 1.0.2-beta1. The Note includes corrections for ASE, IQ, SQL Anywhere, Afaria, Mobile Secure Cloud and other products.

Finally, although Note 2053768 is rated as medium priority, the rating for the underlying CVE vulnerability carries the highest level of severity in terms of impact and exploitability . The vulnerability is also relatively non-complex, requires no authentication, and could be exploited to provoke a denial of service, escalate privileges and access and modify data. The affected component is the NetWeaver Gateway for Microsoft, responsible for integrating Microsoft applications with SAP systems. Customers are advised to upgrade to the latest version of the .NET framework to address the vulnerability.

Appendix: SAP Security Notes, September 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2035923	SD-BIL-IV-PC	Missing authorization check in SD Credit cards
HIGH	2036547	MOB-SYC-SAP	Security mitigation instructions for Agentry 6.1.3
HIGH	2037197	AP-MD-BP	Missing authorization check in AP-MD-BP
HIGH	2039905	BI-BIP-SCH	Missing authorization check in BI-BIP-SCH
HIGH	2042074	MOB-SYC-SAP-WM	Potential information disclosure in MOB-SYC-SAP-WM and MOB-SYC-SAP-SM
HIGH	2042338	FS-CM	Missing authorization check in FS-CM
HIGH	2043506	SV-SMG-DIA	Solution Manager File System Brower - Restrict file content access
HIGH	1852847	BC-WD-JAV	Directory traversal in BC-WD-JAV
HIGH	2013080	MFG-ME	Missing authorization check in standalone POD in Manufacturing Execution
HIGH	2015232	XX-PART-OPT-INV	Missing authorization check in XX-PART-OPT-INV
HIGH	1908631	PY-NPO	Code injection vulnerability in PY-NPO
HIGH	1808384	SBO-IMCE-COM	Unauthorized modification of stored content in B1A
HIGH	1971397	BW-BEX-OT	Missing authorization check in BW-BEX-OT
HIGH	1979454	BC-ABA-SC	Missing authorization check in Batch Input Recorder
HIGH	1984050	SBO-CLD	Unsecured data transmission method in B1Cloud
HIGH	2026763	CA-WUI-UI-TAG	Unauthorized modification of stored content in webcuif
HIGH	2028904	BC-MID-ICF-LGN	Cross-Frame Scripting protection in SAP ABAP HTTP logon application
HIGH	2030775	SRM-CAT-MDM	Missing Authentication Check In Utilities Application Included In The SRM-MDM Catalog
MEDIUM	1872638	CRM-MKT-MPL-TPM-PPG	Code injection vulnerability in CRM-MKT-MPL-TPM-PPG
MEDIUM	1835691	CRM-MKT-MPL-TPM-PPG	Code injection vulnerability in CRM-MKT-MPL-TPM-PPG
MEDIUM	1810405	EHS-SAF	Possible change/disclosure of persisted data in EH&S
MEDIUM	2057196	IS-B-BCA-AM	Missing authorization check in IS-B-BCA-AM
MEDIUM	1880561	FS-AM-PLM	Potential disclosure of persisted data in FS-AM-PLM
MEDIUM	2039924	MOB-SYC-SAP-WM	Missing authentication check in file sharing feature of IOS for SAP Work Manager app

Appendix: SAP Security Notes, September 2014

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	1898548	PA-AS	Potential false redirection of Web site content in EA-HRGXX
MEDIUM	2049371	BC-SYB-ASE	Potential OpenSSL vulnerability (CVE-2014-0224) exposure in multiple SAP Sybase products.
MEDIUM	2053768	OPU-GW-DT-VS	Vulnerability in .NET Framework Could Allow Elevation of Privilege
MEDIUM	2035310	FI-GL-GL-ACE	Switchable authorization check in FI-GL-GL-ACE
MEDIUM	1989060	FI-LA	Switchable authorization check in FI-LA in S_XB7_96000248, *249, *239
MEDIUM	1992822	BW-BEX-ET-WEB	Unauthorized modification of displayed content in BW-BEX-ET-WEB
MEDIUM	2024315	XX-CSC-BG-FI	User-driven dynamic procedure calls vulnerability in C-CEE add-on
LOW	2049141	BC-BMT-WFM	Potential information disclosure relating to Business Workflow
LOW	2054566	BC-BMT-WFM-DEF	Potential disclosure of user information

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