ADVISORY

Layer Seven Security

SAP Security Notes

February 2014

SAP Security Notes

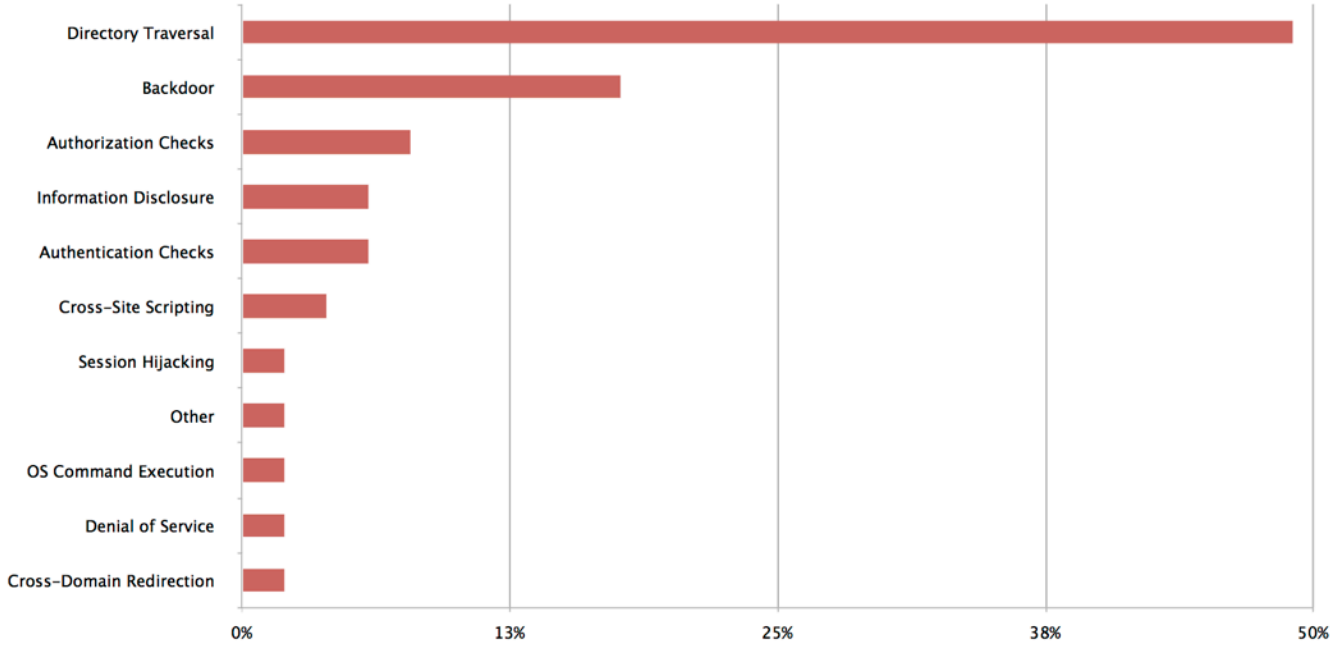
February 2014

SAP's first Hot News security patch of 2014 deals with a crucial operating system command execution vulnerability in AS Java. Note 1963100 contains corrections to disable OS commands that can be executed in a CTC application by invoking a specific URL. Since the vulnerability enables attackers to execute any OS command, it could lead to the complete compromise of SAP systems. The invoker servlet should be disabled when implementing the corrections if it is still enabled (refer to Note 1445998).

Almost half of last month's patches relate to directory traversal vulnerabilities in components of Financial Accounting that could enable attackers to write malicious files to SAP servers impacting the integrity and availability of SAP data and system resources. The relevant corrections to validate physical file names against logical files names can be implemented through support packages or through Notes using the Note Assistant.

There were also a high number of Notes released in February to remove hardcoded username and password combinations in multiple areas of SAP. The combinations provide a backdoor to sensitive functions and could lead to the escalation of privileges. The affected areas include Bank applications in Enterprise Central Component (ECC) (Note 1795463), Project Systems (Note 1791081), SAP Industry Solutions for Oil & Gas (Note 1920323), Production Planning (1789569) and the Computing Center Management System (CCMS) (Note 1911174).

Note 1942592 introduced an important change to X.509-based logon procedures. X.509 client certificates are passed by Web Dispatchers over a secure channel to Internet Communication Managers (ICMs) within NetWeaver Application Servers to enable logons. Certificate data is contained in the HTTP header transmitted by Web Dispatchers to ICMs.



SAP Security Notes by Vulnerability Type

The trust relationship between Web Dispatchers and ICMs is managed by the parameters icm/HTTPS/trust_client_with_issuer = <issuer> and icm/HTTPS/trust_client_with_subject = <subject>. The implementation of Note 1942592 ensures that certificates are only accepted by ICMs when there is a match based on both issuer and subject.

Customers that have implemented SAP Screen Personas Release 1 should immediately apply the Support Package referenced in Note 1907126. Screen Personas renders SAP GUI screens in Web browsers to provide an enriched and personalized user interface.

The Support Package solves several authentication and password-related vulnerabilities in the add-on by introducing rules for password complexity, enforcing the changing of initial passwords and ensuring that users cannot logon to systems after logout using authentication data stored in the browser cache.

Appendix: SAP Security Notes, February 2014 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	1963100	BC-INS-CTC-RT	Disabling execution of operating system commands using a CTC URL
HIGH	1795463	IS-B-DP	Hard-coded credentials in IS-B-DP
HIGH	1950292	SRM-EBP-CAT	Potential false redirection of Web site content in SRM-EBP-CAT
HIGH	1911174	BC-CCM-MON	Hard-coded credentials in CCMS
HIGH	1791081	PS-ST	Hard-coded credentials in PS-ST and PS-MAT-PRO
HIGH	1789569	PP-CRP-LVL	Hard-coded credentials in capacity leveling.
HIGH	1945300	QM-IM-RR	Missing whitelist check in QM-IM
HIGH	1860923	BC-BMT-WMD	Unauthorized modification of displayed content in the Workflow Modeler
HIGH	1768049	XX-CSC-BR	Hard-coded credentials in XX-CSC-BR
HIGH	1830024	BC-SRV-COM-FTP	Update #1 to Security Note 1605054
HIGH	1920323	IS-OIL-DS-TSW	Hard-coded credentials in IS-OIL-DS-TSW
HIGH	1915873	BC-UPG-TLS-TLA	Usage of sy-uname in method
HIGH	1914777	CA-WUI-WST	Hard-coded credentials in CA-WUI-WST
HIGH	1913388	BC-DWB-TOO-RTA	Directory traversal in ABAP Runtime Analysis
HIGH	1738965	BW-WHM-DBA-OHS	Hard-coded credentials in Open Hub
HIGH	1942592	BC-CST-IC	ICM check of certificates forwarded by intermediary
MEDIUM	1961947	XX-CSC-SI-FI	Directory traversal in /CCEE/FISIP
MEDIUM	1961948	XX-CSC-SI-FI	Directory traversal in /CCEE/FISIRFEBKA00
MEDIUM	1961949	XX-CSC-RS-FI	Directory traversal in /CCEE/RSFI_EXPORT_GL_LINE
MEDIUM	1961950	XX-CSC-SI-FI	Directory traversal in /CCEE/SAPCE_TABLES_MIGRATION
MEDIUM	1961951	XX-CSC-SI-FI	Directory traversal in /CCEE/SIFI_CASH_SALES_REPORT
MEDIUM	1961952	XX-CSC-SI-FI	Directory traversal in /CCEE/SIFI_EXPORT_GL_LINE
MEDIUM	1961993	XX-CSC-SI-FI	Directory traversal in /CCEE/SIFI_RFASLM00_SI
MEDIUM	1961994	XX-CSC-SI-FI	Directory traversal in /CCEE/SIFI_RFEBBART00

Appendix: SAP Security Notes, February 2014 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	1961995	XX-CSC-SI-FI	Directory traversal in /CCEE/SIFI_RFEBBART01
MEDIUM	1964200	XX-CSC-BG-FI	Directory traversal in Program /BGLOCS/VATREPORT07
MEDIUM	1964202	XX-CSC-LT-FI	Directory traversal in Invoice Register for Lithuania
MEDIUM	1953935	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFI_RFASLD11B
MEDIUM	1953936	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFIRFUVDE07N
MEDIUM	1953937	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFIRFUVDE2012
MEDIUM	1953939	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFI_D205_MERGE_XML
MEDIUM	1953940	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFI_RGCBILA0
MEDIUM	1953941	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFI_VIES_390_XML
MEDIUM	1953942	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFI_VIES_394
MEDIUM	1953973	XX-CSC-RO-FI	Directory traversal in /CEECV/ROFI_VIES_394_XML
MEDIUM	1953974	XX-CSC-RO-FI	Directory traversal in /CEECV/RO_ANN_FS_EXPORT
MEDIUM	1953975	XX-CSC-RS-FI	Directory traversal in /CCEE/YUFI_RFEBHALC00
MEDIUM	1961946	XX-CSC-SI-FI	Directory traversal in /CCEE/FISIFP_1450
MEDIUM	1783807	CA-CL-SEL	Missing authorization checks in CA-CL
MEDIUM	1883543	CA-MDG-ML	Directory traversal in CA-MDG-ML
MEDIUM	1964201	XX-CSC-EE-FI	Directory traversal in INTRASTAT: File Creation for Receipt/ Dispatch - Estonia Transaction /CEECV/BED
MEDIUM	1905408	BI-BIP-SDK	Potential denial of service in BI-RA-CR
MEDIUM	1781171	BC-WD-JAV	ClickJacking vulnerability in WebDynpro Java
MEDIUM	1846438	BC-JAS-WEB	Unauthorized use of application functions in AS Java
MEDIUM	1939673	EPM-BPC-NW-ADM-DIM	Potential information disclosure relating to planning or consolidation transaction data
MEDIUM	1939334	BC-CCM-SLD	Potential information disclosure relating to Web AS ABAP
MEDIUM	1922154	EPM-BPC-NW-WEB	Potential information disclosure relating to logon information
MEDIUM	1942332	EPM-BPC-NW-WEB-ADM	potential XSS vulnerability in BPC 75 NW Web
MEDIUM	1911319	FS-RI	Missing authorization check in FS-RI
MEDIUM	1907126	BC-PER-RT-SIL	Logout functionality / Password complexity and change
MEDIUM	1716640	FS-RI	Missing authorization check in FS-RI

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