ADVISORY

Layer Seven Security

SAP Security Notes

January 2014

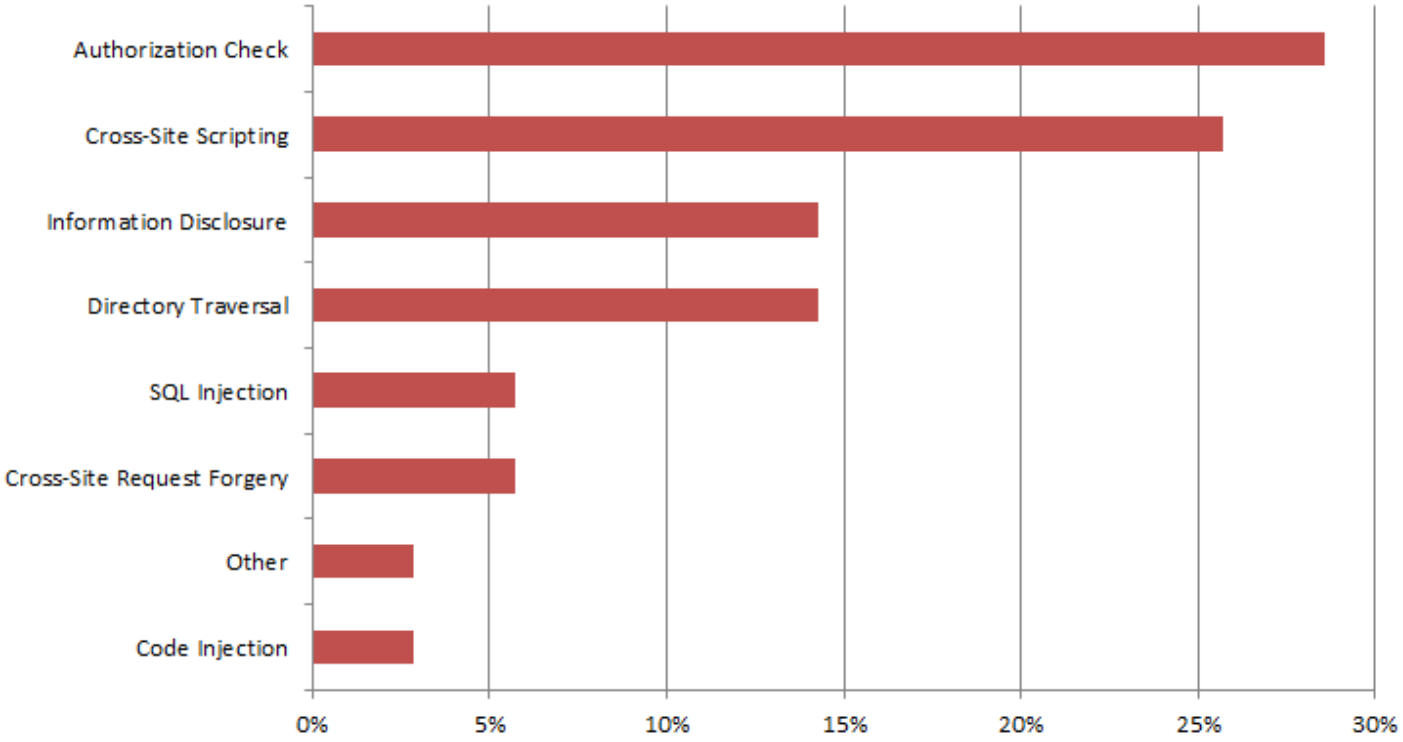
SAP Security Notes

January 2014

One of the most important Security Notes released by SAP in January patches several vulnerabilities in Portal Site Management, a Web content management solution designed to integrate documents and other resources across multiple portals. Portal Site Management is developed by SAP in partnership with OpenText, a global leader in Enterprise Information Management (EIM) software. Note 1939662 deals with Cross-Site Request Forgery (XSRF), information disclosure and directory traversal vulnerabilities in the Portal Site Management Server that could lead attackers to execute administrative functions without authentication or authorisation, discover information related to session variables, and traverse the file system of the Management Server. Aside from implementing the patch delivered with the Note, customers should upgrade to version 11.1 of the Management Server and ensure that the Server is not publically accessible. For detailed information, refer to the OpenText Web Site Management System Overview Guide.

Note 1865109 introduces an important change to Diagnostics Agents used to monitor satellite systems through Solution Manager. The correction packaged with the Note removes the elevated privileges assigned to users required by Agents. This greatly reduces the impact of targeted attacks against Agents and eliminates the risk of attackers connecting to SAP systems using the administrative privileges of compromised users.

Note 1886051 deals with a dangerous code injection vulnerability in the Database Interface of Business Warehouse (BW-BEX-OT-DBIF). The Interface includes an analytic engine responsible for processing information requests and a data manager that converts requests into SQL statements. Customers are advised to implement the relevant Support Package referenced in the Note to resolve a vulnerability in the component that could enable attackers to execute arbitrary code, modify, view and



SAP Security Notes by Vulnerability Type

delete data, create new users with administrative privileges and provoke a denial of service.

Note 1932505 patches a reflected cross-site scripting vulnerability in both the desktop and HTML versions of the NetWeaver Business Client (NWBC). The vulnerability is caused by insufficient encoding of input parameters within a specific web service and could lead to the compromise of SAP systems through the theft of user credentials.

Customers that have deployed the Live Auction Cockpit in Supplier Relationship Management (SRM) to manage real-time bids should implement Note 1916560. This patches a vulnerability that could effect the integrity of the bid process through the unauthorised disclosure of information related to bidders.

Finally, all customers should apply Notes 1917381 and 1918333 which deal with missing authorization checks in critical Basis areas related to the maintenance of user profiles and batch processing.

Appendix: SAP Security Notes, January 2014 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	1966829	CRM-BF-CFG	Update 1 to security note 1591517
HIGH	1828885	SV-SMG-DIA-APP	Potential information disclosure relating to Managed systems
HIGH	1943958	SRM-EBP-WFL	Update 1 to security note 1903266
HIGH	1943852	IS-B-BCA	Missing authorization check in IS-B-BCA
HIGH	1942424	SV-SMG-ASU	Missing authorization check in SV_SMG-ASU
HIGH	1884596	BC-SRV-BTF	Unauthorized modification of stored content in Business Workplace
HIGH	1886051	BW-BEX-OT-DBIF	Code injection vulnerability in BW-BEX-OT-DBIF
HIGH	1754772	CRM-ISA-TEC	Update 1 to security note 1744747
HIGH	1894049	BC-UPG-SLM	Potential information disclosure relating to SLM
HIGH	1898046	BW-SYS-DB-HDB	Potential modif./disclosure of persisted data in BW-SYS-DB
HIGH	1956096	BW-WHM-DBA	Missing whitelist check in BW-WHM-DBA
HIGH	1939662	XX-PART-OPT-PSM	Unauthorized use of application functions in SAP Portal Site Management by OpenText XX-PART-OPT-PSM
HIGH	1865109	SV-SMG-DIA	Potential information disclosure in Diagnostics Agents
HIGH	1788080	BC-XI-IBD	PI SEC: Unauthorized modification of displayed content in PI
HIGH	1910914	BC-DOC-HLP	Missing authorization check in BC-DOC-HLP
HIGH	1917381	BC-CCM-CNF-PFL	Missing authorization check in Profile Maintenance
HIGH	1918333	BC-CCM-BTC	Missing authorization check in SAP Background Processing
HIGH	1924853	BC-CST-IC	Unauthorized modification of displayed content in ICM
HIGH	1931399	BI-BIP-INV	Unauthorized modification of displayed content in BI-BIP-INV
HIGH	1932505	BC-FES-BUS	Unauthorized modification of displayed content in NWBC
HIGH	1963303	CRM-IC-BRO	Update#1 to Security Note 1675484
MEDIUM	1833327	BC-SRV-ADR	Potential disclosure of persisted data in BC-SRV-ADR
MEDIUM	1915908	FS-RI-RMN	Missing authorization check in FS-RI
MEDIUM	1787906	BC-BSP	Unauthorized modification of displayed content in BSP pages

Appendix: SAP Security Notes, January 2014 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	1769611	PY-SE	Directory traversal in PY-SE
MEDIUM	1771706	PY-FI	Directory traversal in PY-FI
MEDIUM	1777988	PY-SE-PS	Directory traversal in PY-SE-PS
MEDIUM	1942432	FI-LA	Missing authorization check in FI-LA
MEDIUM	1949046	SV-SMG-SDD	Broken authorization check
MEDIUM	1841786	XAP-MBA-MSO	Unauthorized use of application functions in MSON
MEDIUM	1916560	SRM-LA	Potential information disclosure relating to bidders
MEDIUM	1916861	CA-WUI-UI-TAG	Unauthorized modification of displayed content in CA-WUI-UI
MEDIUM	1922547	EP-PIN-WD	Missing authentication check in NW EP iView Wizard
MEDIUM	1940022	XX-CSC-RU-FI	Missing authorization check in J3RFGTDINT
MEDIUM	1782959	XX-CSC-BR	Directory traversal in XX-CSC-BR

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