Layer Seven Security

ADVISORY

SAP Security Notes

January 2015

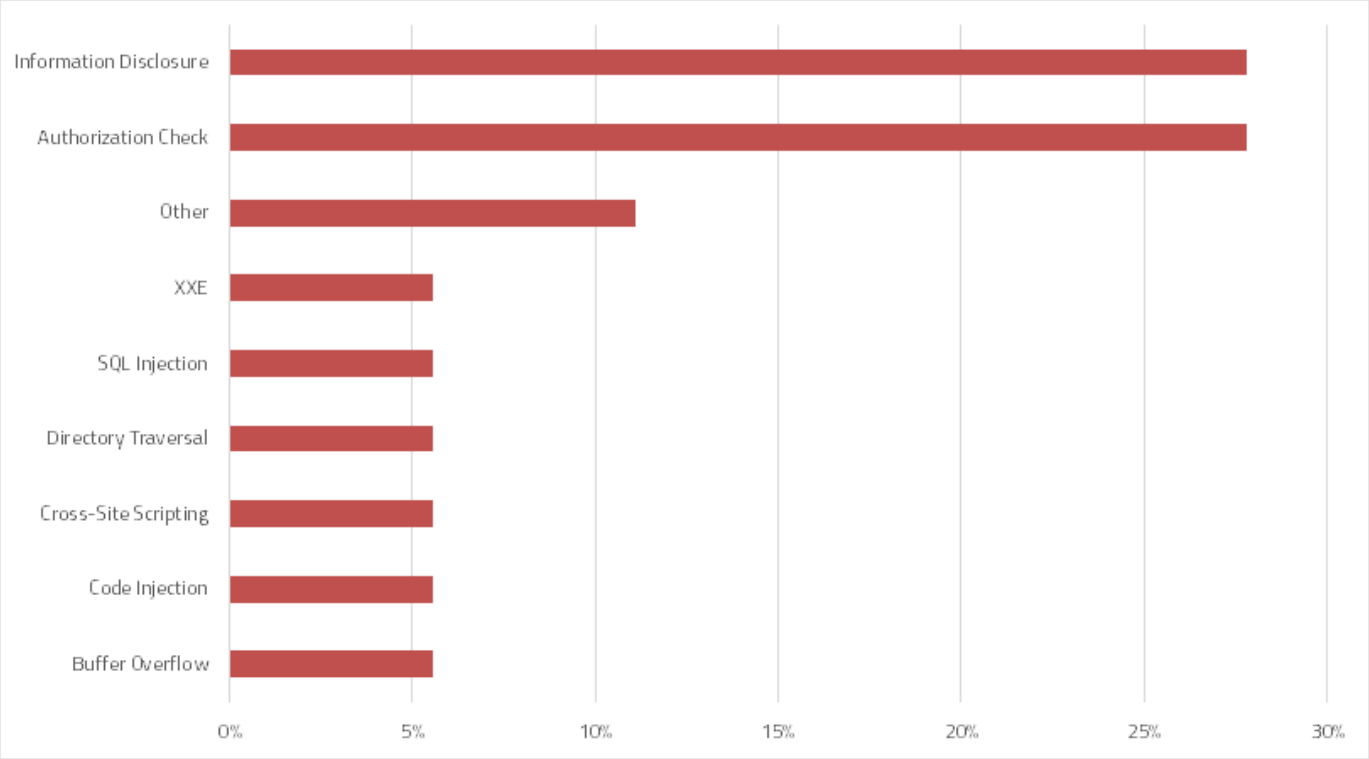
SAP Security Notes

January 2015

The most critical patch released by SAP in January introduced two new parameters to counteract the POODLE vulnerability in the AS Java. Note 2094598 enables customers to specify the versions of the SSL/TLS protocol supported by the J2EE using the properties SSL_VERSION_MIN and SSL_VERSION_MAX. The respective default values are TLS10 and TLS11. Therefore, the standard configuration of AS Java will not support the vulnerable SSLv3 protocol once the corrections packaged in the relevant support packages referenced in the Note are applied.

SAP released corrections for multiple vulnerabilities in components of the Workforce Scheduling and Optimization solution by ClickSoftware. The solution supports real-time and mobile resource allocation and integrates directly with ERP, CRM and other platforms. Note 2111169 includes corrections for high-risk code injection, privilege escalation and authentication bypass weaknesses in components such as ClickMobile and ClickSchedule. Customers should install the .msi files included in the Note to remove the underlying vulnerabilities in the ClickMobile MiddleTier server and the ClickSchedule web service.

Note 1985387 deals with an information disclosure vulnerability impacting SAP Solution Manager that could lead to the exposure of usernames and passwords for connections supporting Diagnostics Agents that transmit data from managed systems. The vulnerability is caused by the logging of username and password combinations in log files generated by specific versions of SAP installers such as sapinst and Software Provisioning Manager (SWPM). Customers are urged to change the password for



SAP Security Notes by Vulnerability Type

SMD_ADMIN, SMD_AGT or other users that are configured for connections between Solution Manager systems and Diagnostic Agents. Deletion of the installer log files is also recommended. The log files are typically written to the C:\Program Files\sapinst_instdir directory in Windows systems and the /tmp/sapinst_instdir directory in Linux/UNIX systems.

Note 1605531 patches a similar vulnerability in the Master Data Management (MDM) application Global Data Synchronization (GDS) used to align data objects and attributes in inter-company and cross-company supply chains. The Note removes the storage of plain-text user credentials in the memory of the GDS server. The credentials may be accessed by users with access to the operating system of the server.

Finally, Note 2065073 improves the authorization checks performed during the execution of system traces in order to prevent unauthorized users accessing sensitive information in authorization, kernel, database, RFC and table traces using transaction ST01. The Note introduces an additional check for the authorization object S_ADMI_FCD used for system administration with the value ST0R which controls the ability to analyze system logs.

Appendix: SAP Security Notes, January 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2094598	BC-JAS-SEC-CPG	Fixing POODLE SSLv3.0 Vulnerability in AS Java
HIGH	2120370	BI-BIP-AUT	Update 1 to Security Note 2001109
HIGH	2113333	BC-SYB-ASE	Multiple SQL injection vulnerabilities in SAP ASE
HIGH	2111169	XX-PART-CLK	Security Vulnerabilities in ClickSoftware Applications
HIGH	2109565	HAN-DB	Potential information disclosure relating to IMPORT FROM statement in SAP HANA
HIGH	2000401	IS-A-DP	Missing authorization check in IS-A-DP
HIGH	1985387	SV-SMG-INS-AGT	Potential information disclosure relating to SAP Solution Manager
HIGH	2016638	BC-TWB-TST-ECA	Untrusted XML input parsing possible in BC-TWB-TST-ECA
HIGH	2065073	BC-CST-LL	Missing authorization check in System Trace
HIGH	2098906	HAN-AS-XS	Code injection vulnerability in SAP HANA XS
MEDIUM	2115185	FI-AP-AP-N	Update 1 to Security Note 2030997
MEDIUM	1951171	LO-SPM	Potentially controllable RFC function module for postings in EWM
MEDIUM	1964201	XX-CSC-EE-FI	Directory traversal in INTRASTAT: File Creation for Receipt/Dispatch - Estonia Transaction /CEECV/BED
MEDIUM	1978131	EP-PCT-PUR-BP	Missing authorization check in EP-PCT-PUR-BP
MEDIUM	2090692	BC-SEC	Security vulnerability in ICM content filter [sapcsa]
MEDIUM	1937544	OPU-GW-CORE	Unauthorized modification of displayed content in User Self Service
MEDIUM	1710213	FS-RI-B	KORR: Possible disclosure of persisted data in FS-RI
MEDIUM	1605531	MDM-GDS	Credentials are stored in memory by SAP MDM GDS 2.1

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