Layer Seven Security

ADVISORY

SAP Security Notes

July 2014

SAP Security Notes

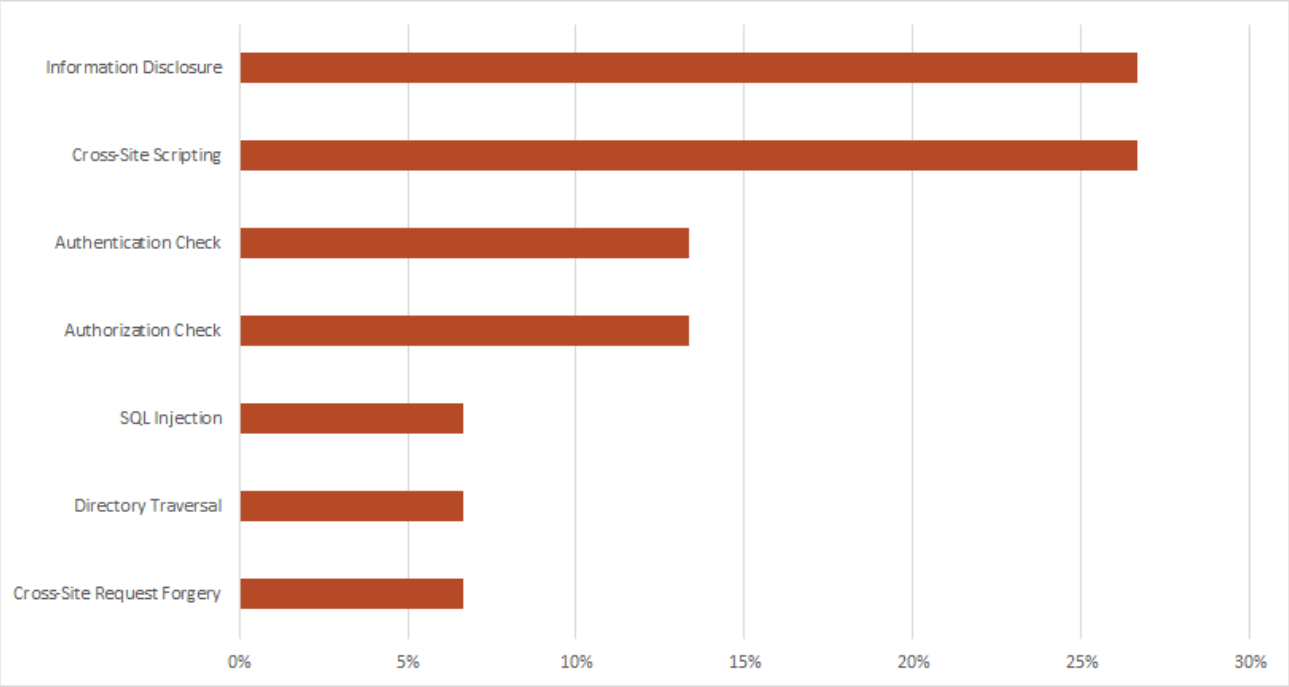
July 2014

SAP released an unusually high number of Security Notes in July to address information disclosure vulnerabilities that could lead to the compromise of sensitive information including system passwords. This includes vulnerabilities in Web Container and HTTP Services that could expose information related to installed products, versions and source codes in AS Java (Notes 1867507 and 1985445). Both services are an integral component of AS Java's Web Container which provides the runtime environment for servlets, JSPs and JSFs.

Note 1820305 contains corrections to remove the option to store passwords for LDAP directory servers in simple memory and transferring passwords to the Secure Store. Without the implementation of the corrections, passwords are vulnerable to discovery using a database table lookup.

Note 2030625 recommends encryption for cluster, endpoint and security configuration data using MD5 and special characters to prevent the discovery of passwords related to the administrative console of the Sybase Mobile Platform. The Platform provides a framework for the development of applications that connect data in enterprise databases and systems to mobile devices. MD5 is a widely-deployed cryptographic algorithm used to generate hash values to secure sensitive data in storage. It is also used to secure certain code versions of SAP passwords.

Other important patches released by SAP include corrections to remove an authentication bypass vulnerability in the Production Operator Dashboard of SAP Manufacturing when accessed via a standalone URL. Note 1987927 deals with a program error that keeps sessions alive even after users have selected the logout option. This presents an acute risk in manufacturing environments since workstations are often shared between multiple users.



SAP Security Notes by Vulnerability Type

SAP also addressed a similar but lower-priority vulnerability in the Fiori Launchpad which provides an interface to Fiori apps for mobile and desktop users. The Launchpad renders a role-based home page for each user with tiles for the business applications that are authorized for the user. Note 2010502 contains detailed instructions to remove weaknesses in session security impacting connections through the SAP Gateway, HANA and other systems that are not supported by the Launchpad's logout feature. The corrections are designed to enforce proper session termination for connections to ABAP applications and systems using REST or OData that do not load remote catalogs.

Appendix: SAP Security Notes, July 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2017050	BC-CUS-TOL-HMT	Update 1 to Security Note 1971238
HIGH	2011169	HAN-LM-APP	Unauthorized use of application functions in SAP HANA application lifecycle manager
HIGH	1867507	BC-JAS-WEB	Potential information disclosure relating to AS Java
HIGH	1962104	BC-WD-JAV	Unauthorized modification of stored content in BC-WD-JAV
HIGH	1988956	BC-BSP	Unauthorized modification of displayed content in BSP
HIGH	1987927	MFG-ME	Security risk with logout feature in standalone POD
HIGH	2036562	MOB-AFA	Potential modification of persisted data in Afaria Server
MEDIUM	2030625	MOB-SUP-SCC	Potential information disclosure relating to password used in SUP2.X admin tooling
MEDIUM	1840515	PE-LSO-LPO	Unauthorized modification of displayed content in LSOFE
MEDIUM	2010502	CA-UI2-INT-FE	Missing Authentication in SAP Fiori Launchpad
MEDIUM	1936262	SV-SMG-ASU	Directory traversal in SV-SMG-ASU
MEDIUM	1820305	BC-SEC-DIR	Potential information disclosure relating to passwords: LDAP
MEDIUM	1985445	BC-JAS-WEB	Potential information disclosure in Web Container
MEDIUM	1998770	BC-BMT-WFM	Unauthorized change of stored content through manipulation of BC-BMT-WFM
LOW	2019843	FIN-FSCM-TRM-TM-IS	Missing authorization check in FIN-FSCM-TRM-TM-IS

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