Layer Seven Security

ADVISORY

SAP Security Notes

April 2015

SAP Security Notes

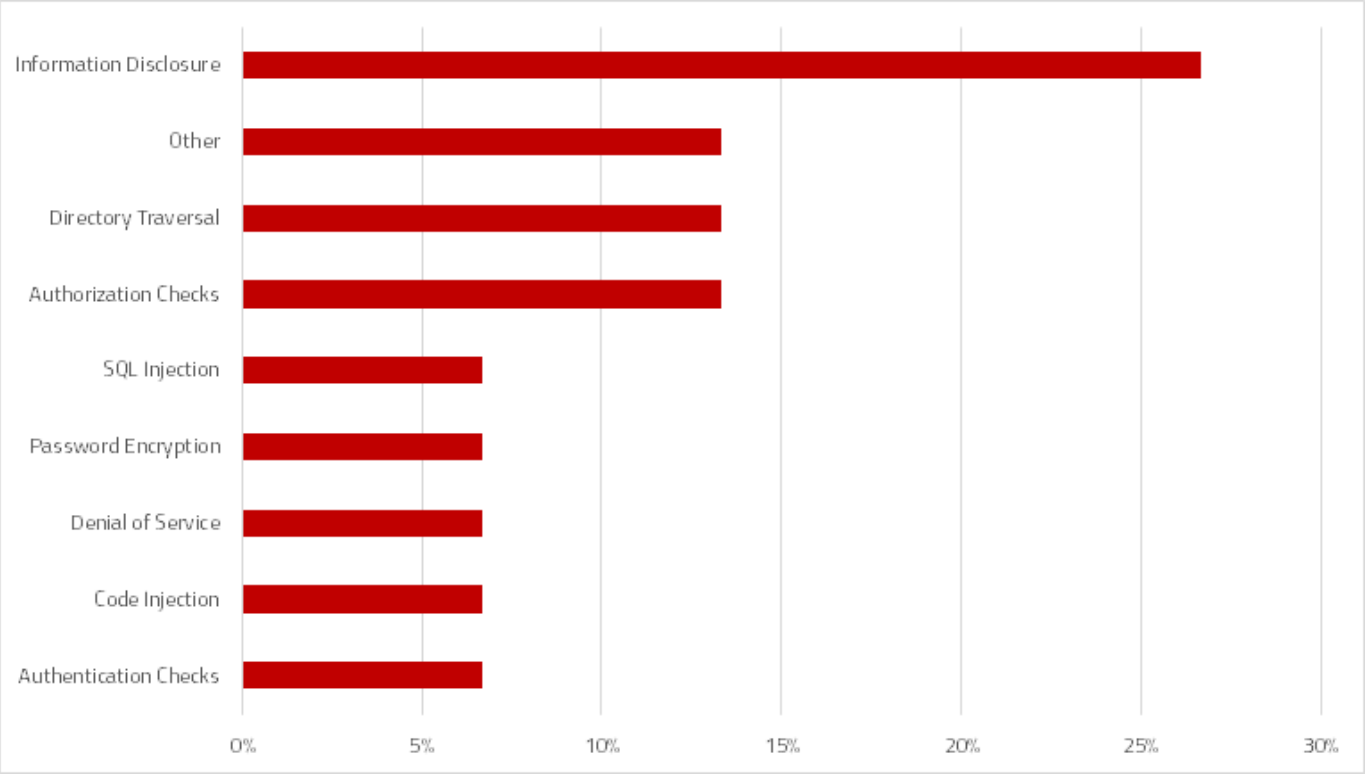
April 2015

The most critical patch released by SAP in April corrected a missing authentication check in Sybase Adaptive Server Enterprise (ASE). ASE is an RDBMS often used in data-intensive environments. Note 2113995 strongly recommends upgrading to the latest available SP levels for ASE versions 15.7 and 16.0.

ASE and other Sybase products were impacted by the FREAK vulnerability reported by cryptographers earlier this year. FREAK or Factoring Attack on RSA-EXPORT Keys enables attackers to decrypt client-server communications secured using the SSL/ TLS protocol. The vulnerability arises in clients that degrade from strong RSA to the weaker export grade RSA which limits the length of encryption keys to 512-bits or less. The vulnerability can be removed by disabling server-side support for export suites. Note 2152703 lists the fixed versions of Sybase products including ASE, SQL Anywhere and Mobile Platform.

Note 2137898 removes a high priority missing authorization check in Sales Documents (SD-SLS). Sales Documents is a core application in the Sales and Distribution module of SAP ERP. It is used to generate and process inquiries, quotations, orders, agreements, invoices and other documents. Customers should install the relevant support package for the applicable release level of the software component SAP_APPL.

Note 1849842 also patches a high priority vulnerability in a crucial SAP component. It improves session logging and tracing functions to prevent the disclosure of sensitive information related to the Payment Methods component in Web



SAP Security Notes by Vulnerability Type

Channel Experience Management used to power online commerce.

Although SAP has assigned a low priority level to Note 2003727, the implementation of the relevant J2EE Engine SP patch is recommended since it removes support for weaker hash algorithms vulnerable to attacks using password cracking tools. UME password hashes are stored in the UME_STRINGS table and generally secured using the SSHA1 algorithm. It should be noted, however, that none of the hash algorithms supported by SAP systems are completely invulnerable to password cracking attempts.

Other important patches released in April include Note 2140700 which removes a memory corruption flaw that can be exploited to crash the HDBSQL client for SAP HANA, Note 2097534 which deals with an injection vulnerability in the Business Rules Framework for CRM, and finally, Note 2094830 which improves encryption levels for username and password combinations stored in iOS and Android devices for the SAP Mobile Platform. Attackers may be able to access encrypted credentials stored in secure locations within jailbroken/ rooted devices.

Appendix: SAP Security Notes, April 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2113995	BC-SYB-ASE	Missing authentication check in SAP ASE
HIGH	2137898	SD-SLS	Missing authorization check in SD-SLS
HIGH	2140700	HAN-DB-CLI	Potential termination of HANA client (hdbsql)
HIGH	2097534	CRM-BF-BRF	Code injection vulnerability in CRM-BF-BRF
HIGH	2094830	MOB-SUP-ODP	Potential information disclosure relating to mobile onboarding
HIGH	2067830	BC-WD-JAV	Security issue with AV protection in webdynpro file upload
HIGH	2152703	BC-SYB-SQA	Fixing FREAK vulnerability in multiple SAP Sybase products
HIGH	1849892	WEC-APP-PAY	Potential information disclosure relating to WEC-APP-PAY
MEDIUM	1783772	XX-CSC-AR	FI: Potential Directory Traversal - Argentina
MEDIUM	1793635	XX-CSC-AR	Directory traversal in XX-CSC-AR
MEDIUM	2153625	LO-SLC	Potential disclosure of persisted data in SAP CPQ Solution Configuration
MEDIUM	1979543	BC-JAS-SEC-LGN	Potential Disclosure of AS Java Related Information
MEDIUM	2125925	SD-MD-CM	Missing authorization check in SD-MD-CM
MEDIUM	2084037	BC-MID-RFC-SDK	Potential information disclosure relating to RFC SDK
LOW	2003727	BC-JAS-SEC-UME	Password Hash Algorithm in UME

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