Layer Seven Security

ADVISORY

SAP Security Notes

June 2015

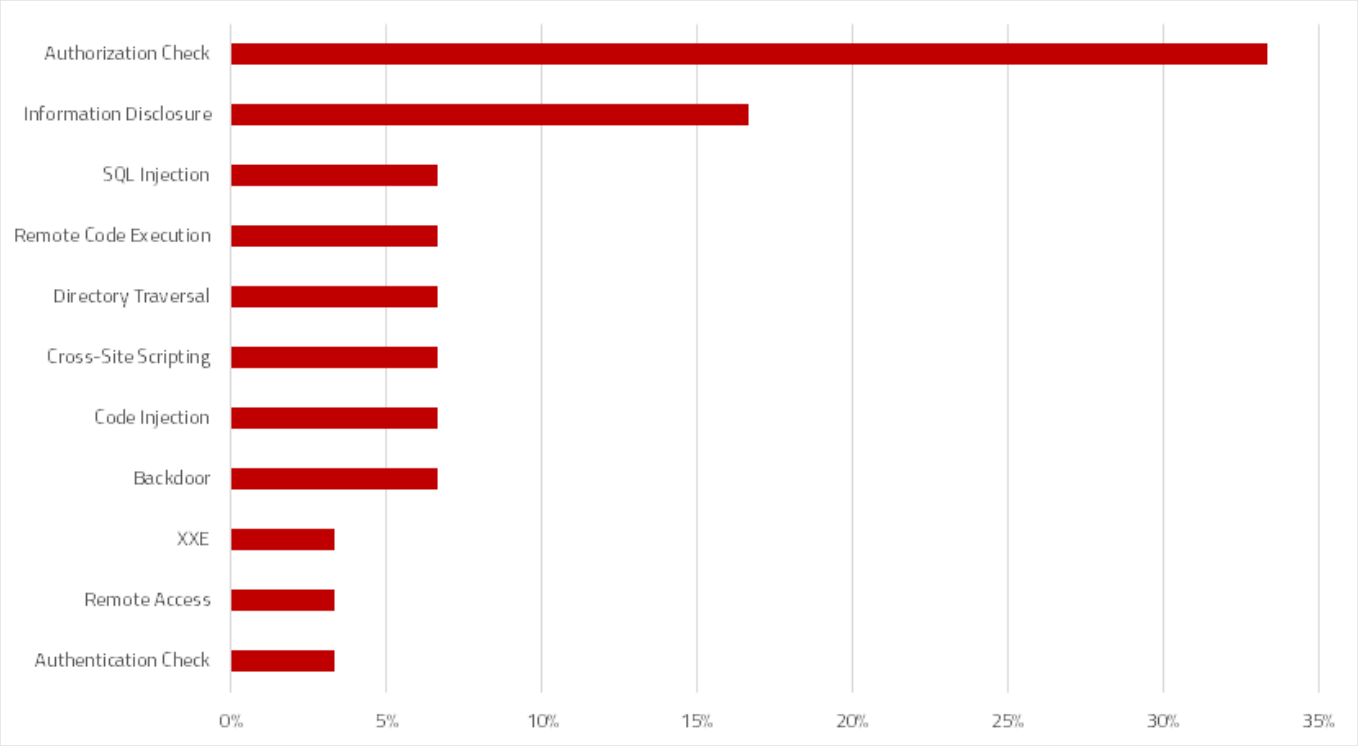
SAP Security Notes

June 2015

Security researchers disclosed a dangerous vulnerability in the SAP HANA platform at the Black Hat conference in June. The vulnerability effects installations with default master keys for the SSFS secure storage. The keys are used to encrypt user passwords and root encryption keys. The identical default key is used for every installation. Therefore, this vulnerability could be exploited to decrypt passwords and other sensitive information stored within the persistent memory of HANA.

Following the public disclosure of the vulnerability, SAP issued an announcement to prompt SAP customers to follow recommendations within the HANA Security Guide for the changing of the default SSFS master key. Detailed instructions for changing the key are provided within the Administration Guide for HANA and Note 2183624. New master keys can be generated using the rsecssfx program stored in /usr/sap/<sid>/HDB<instance>/exe. Once the key is generated, the SSFS should be re-encrypted using the new key and stored in the recommended file location. The SSFS key for the hdbuserstore can also be changed to secure connection information.

Although the vulnerability addressed by Note 2183624 enjoyed a great deal of press attention, it was by no means the most highly-rated security risk addressed by SAP in June. This honor goes to Note 2181338 which extends the coverage of the missing authentication check addressed by Note 2113995 in the Sybase ASE database platform to include version 15.0. The correction instructions in Note 2113995 have been updated accordingly.



SAP Security Notes by Vulnerability Type

Other important patches released last month include Notes 2152703 and 2163306 which address the FREAK vulnerability impacting SSL/ TLS implementations in the CommonCryptoLib, SAPCRYPTOLIB and multiple Sybase products including the Mobile Platform and SQL Anywhere. FREAK is an acronym for the Factoring Attack on RSA-EXPORT Keys that can be exploited by attackers to decrypt secure client-server communications.

Note 1971516 removes a code injection vulnerability in the Service Data Download function of the ST-PI plugin used for data collection and analysis. The vulnerability can be abused to, among other things, modify or delete data, create users with elevated privileges, and carry out denial of service attacks by running malicious code.

Note 2151237 addresses a similar vulnerability in SAP GUI for Windows that could lead to the compromise of the SAP client. Since SAP GUI patches are applied directly to installation servers or front ends, customers should follow the patching instructions in the SAP GUI Installation Guide or Note 535308.

Finally, Notes 2139366, 1997734 and 2084143 address high risk program errors effecting remote function calls. This includes missing authorization checks for the RFC runtime and destination maintenance. It also includes a potential bypass of Unified Connectivity safeguards when multiple function modules are invoked by a single program.

Appendix: SAP Security Notes, June 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2181338	BC-SYB-ASE	Update 1 to Security Note 2113995
HIGH	2152703	BC-SYB-SQA	Fixing FREAK vulnerability in multiple SAP Sybase products
HIGH	2183624	HAN-DB-SEC	Potential information leakage using default SSFS master key in HANA
HIGH	2180264	SV-SMG-SDD	Update 1 to security note 1971516
HIGH	1971516	SV-SMG-SDD	Code injection vulnerability in SV-SMG-SDD
HIGH	2181339	BC-SYB-ASE	Update 1 to security note 2152278
HIGH	2181340	BC-SYB-ASE	Update 1 to security note 2155153
HIGH	1594294	XX-CSC-AR	FI: Potential Directory Traversal - Argentina
HIGH	2178874	XX-CSC-AR	Update 1 to security note 1594294
HIGH	2129609	EP-CON-DB	Potential modif./disclosure of persisted data in EP JDBC Connector
HIGH	2139366	BC-MID-RFC	Potential bypass of unified connectivity runtime checks possible in BC-MID-RFC
HIGH	2144333	CRM-LAM	Missing authorization check in CRM-LAM
HIGH	1997734	BC-MID-RFC	Missing authorization check in RFC runtime
HIGH	2151237	BC-FES-GUI	Potential remote code execution in SAP GUI for Windows
HIGH	2155614	SD-SLS	Missing authorization check in SD-SLS, SD-CAS and SD-MD-AM-CMI
HIGH	2156031	BC-ESI-ESF-BSA	Potential information disclosure relating to SADL Runtime
HIGH	2157241	IS-B-BCA-MD	Missing authorization check in IS-B-BCA-MD
HIGH	2157877	SD-CAS-SP	Missing authorization check in SD-CAS-SP
HIGH	2159601	MOB-ONP	SAP Mobile Platform XXE (add repository)
HIGH	2163306	BC-SEC-SSL	Fixing FREAK vulnerability in CommonCryptoLib and SAPCRYPTOLIB
HIGH	2084143	BC-MID-RFC	Missing authorization check in RFC destination maintenance
HIGH	2059659	BC-CUS-TOL-CST	Hardcoded credentials in BC-CUS-TOL-CST
MEDIUM	2043447	SV-SMG-TWB-BCA	Missing authorization check in SV-SMG-BPCA
MEDIUM	2053197	SV-SMG-CM	ChaRM: Missing authorization check in SV-SMG-CM

Appendix: SAP Security Notes, June 2015 Cont.

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2122022	BC-CCM-PRN	Missing authorization check in function RSPO_R_SAPGPARAM
MEDIUM	1997974	CRM-BF-SVY	Unauthorized modification of displayed content in CRM-BF-SVY
MEDIUM	2120721	CEC-MKT-CEI-BF	Unauthorized modification of displayed content in CEC-MKT-CEI-BF / CA-CEI-ADT
MEDIUM	2057982	BC-SRV-DX-DXW	Hardcoded credentials in BC-SRV-DX-DXW
MEDIUM	2099484	FS-PE	Missing authorization check in Payment Engine
LOW	2150197	BC-DWB-TOO-ATF	Potential information disclosure relating to Code Inspector

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