Layer Seven Security

ADVISORY

SAP Security Notes

October 2014

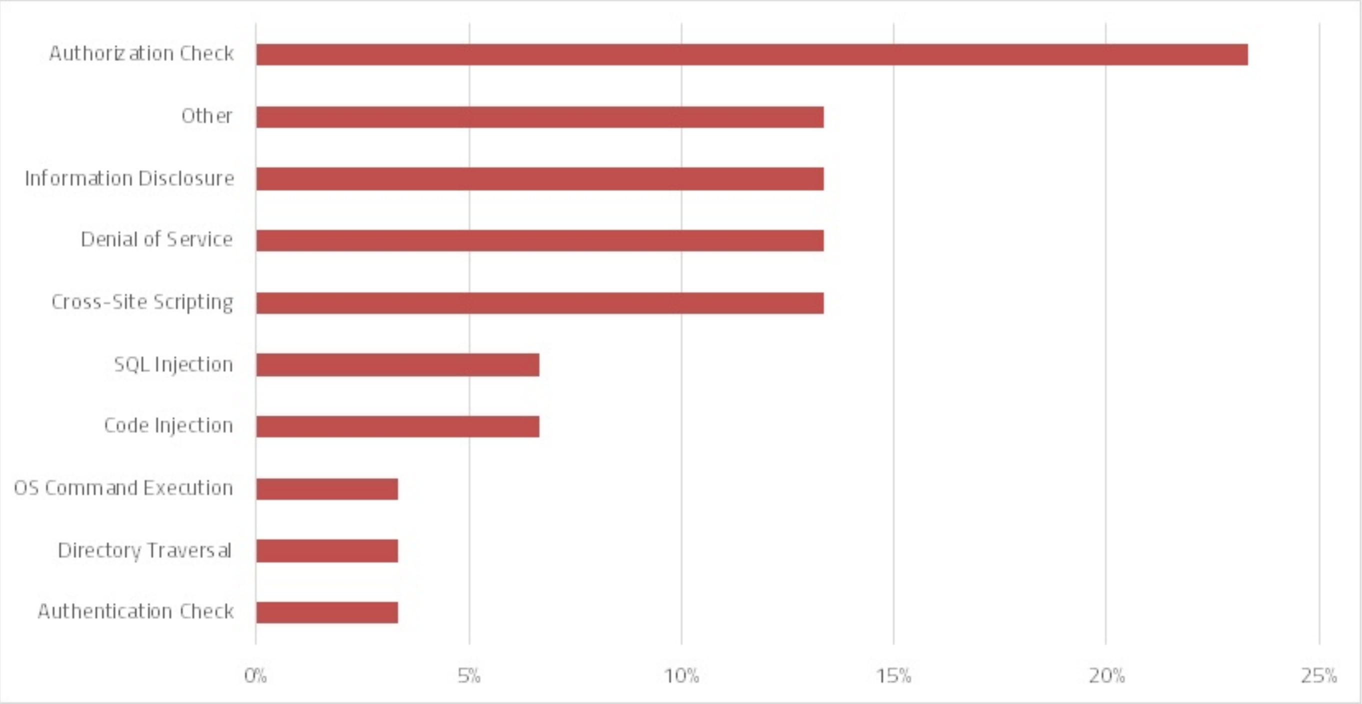
SAP Security Notes

October 2014

There were three important security announcements released by SAP in October. The first related to the ShellShock vulnerability which carried the highest possible severity rating from NIST. ShellShock is a command execution vulnerability impacting a commonly used shell in Linux, UNIX and OS X systems. There are several payloads that are actively exploiting the vulnerability to compromise servers and steal sensitive information through the injection of malicious commands. This includes malware such as PerlBot-A, PerlShl-A, Tsunami-A and PHPFlood-A. ShellShock impacted SAP's cloud infrastructure including Ariba, SuccessFactors and Hybris. Customers with on-premise installations are urged to apply the relevant patches from vendors such as AIX, Solaris, SUSE and RedHat.

The second announcement related to a critical vulnerability in components of SAPCRYPTOLIB, SAPSECULIB and CommonCryptoLib used to support encryption and authentication functions in NetWeaver Application Servers for ABAP and HANA applications. Customers should upgrade the affected libraries to prevent attackers from exploiting the vulnerability by spoofing digital signatures. For NetWeaver AS ABAP, the patch can also be applied through a kernel update (refer to Note 2067859).

The third and final announcement concerned the man-in-the-middle exploit referred to as POODLE (Padding Oracle On Downgraded Legacy Encryption). POODLE attacks clients and servers that support the obsolete and vulnerable SSL 3.0 protocol for transport layer security. This includes some implementations of OpenSSL. The exploit can be patched by enabling support for the signaling cipher suite value TLS_FALLBACK_SCSV to prevent attackers from provoking protocol downgrades from the more secure TLS 1.0 to versions such as SSL 3.0.



SAP Security Notes by Vulnerability Type

Note 2085139 upgraded the priority level of Note 2043404 from medium to very high. The latter included corrections for a code injection vulnerability in the technical infrastructure of SAP CRM. Customers are strongly advised to implement the Java Support Pack attached to the Note.

Note 1936898 implements multiple fixes for security weaknesses in the CRM Mobile Client. It includes restrictions for file permissions, virus checks, encryption, and improved login procedures to address information disclosure and other risks that could be exploited to upload malicious files to servers or read sensitive configuration and authentication data.

Notes 2042845, 2037492 and 1966655 deal with dangerous vulnerabilities in critical components such as the ICM and SAProuter that could lead to a denial of service using specific types of malicious requests to provoke resource exhaustion.

Finally, Note 1686632 introduces a dynamic profile parameter and support for positive whitelists to manage the risks associated with call-backs during synchronous RFC calls. This can be exploited to execute remote-enabled function modules in calling systems from called systems. The security enhancements delivered with this Note and the recommendations in the paper Securing Remote Calls recently released by SAP will be reviewed in detail by Layer Seven Security in a forthcoming blog article. The article can be read at http://layersevensecurity.com/category/blog/.

Appendix: SAP Security Notes, October 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2085139	CRM-ISA-TEC	Update 1 to security note 2043404
HOT NEWS	2043404	CRM-ISA-TEC	Code injection vulnerability in CRM-ISA
HOT NEWS	2067859	BC-SEC	Potential Exposure to Digital Signature Spoofing
HIGH	1906212	BC-SRV-KPR-DMS	Potential command execution in BC-SRV-KPR
HIGH	2050329	FS-AM-IM-IT	Missing authorization check in Posting Items
HIGH	2045176	BC-ESI-WS-JAV-CFG	Update 1 to Security Note 1169248
HIGH	2042845	BC-CST-EQ	Potential denial of service in Enqueue Server
HIGH	2037492	BC-CST-NI	Potential denial of service in SAP Router
HIGH	1686632	BC-MID-RFC	Positive lists for RFC callback
HIGH	1966655	BC-CST	Potential denial of service in ICM
HIGH	1965819	BW-WHM-DBA	Potential modification / disclosure of persisted data in BW-WHM-DBA
HIGH	1936898	CRM-MT	CRM Mobile Client: Security Fixes
HIGH	1986396	BI-RA-WBI	Unauthorized modification of displayed content in BI-RA-WBI
HIGH	1986725	BC-CST-STS	Potential denial-of-service attack against SAP Start Service and SAP Host Agent
HIGH	2010153	EP-PIN-NAV	Unauthorized modification of displayed content in portal page toolbar
HIGH	2018681	BI-BIP-ADM	Missing authentication check in BI-BIP
HIGH	2011395	BI-BIP-ADM	Potential information disclosure relating in BI-BIP-ADM
HIGH	2018682	BI-BIP-ADM	Potential information disclosure relating to BI-BIP
HIGH	2069676	HAN-WDE	Unauthorized modification of displayed content in SAP HANA Web-based Development Workbench
HIGH	2067972	HAN-AS-XS-ADM	Potential modification of persisted data in HANA XS Administration
HIGH	2011396	BI-BIP-ADM	Missing authorization check in BI-BIP-ADM
MEDIUM	2022179	XX-CSC-PT-FICA	Potential disclosure of persisted data in XX-CSC-PT-FICA
MEDIUM	1707816	CA-FS-ECH	Potenzielle Offenlegung von Payload-Daten
MEDIUM	2080679	AP-MD-BP	Missing authorization check in AP-MD-BP

Appendix: SAP Security Notes, October 2014

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2080283	AP-MD-BP	Missing authorization check in AP-MD-BP
MEDIUM	2079818	SRM-EBP-ADM-XBP	Missing authorization check in SRM-EBP-ADM-XBP
MEDIUM	2054616	BC-SEC-AUT	Authority-check not working properly if used without fields
MEDIUM	2052082	EHS-HEA-BD	Directory traversal in EHS
MEDIUM	2076845	PY-XX-PYP	Correction for insecure session handling
MEDIUM	2027997	FIN-FSCM-TRM-TM-TR	Authorization check for RFC in FIN-FSCM-TRM-TM-TR

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

SAP Partner

Layer Seven Security offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Layer Seven Security makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.

This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.