Layer Seven Security

ADVISORY

SAP Security Notes

September 2016

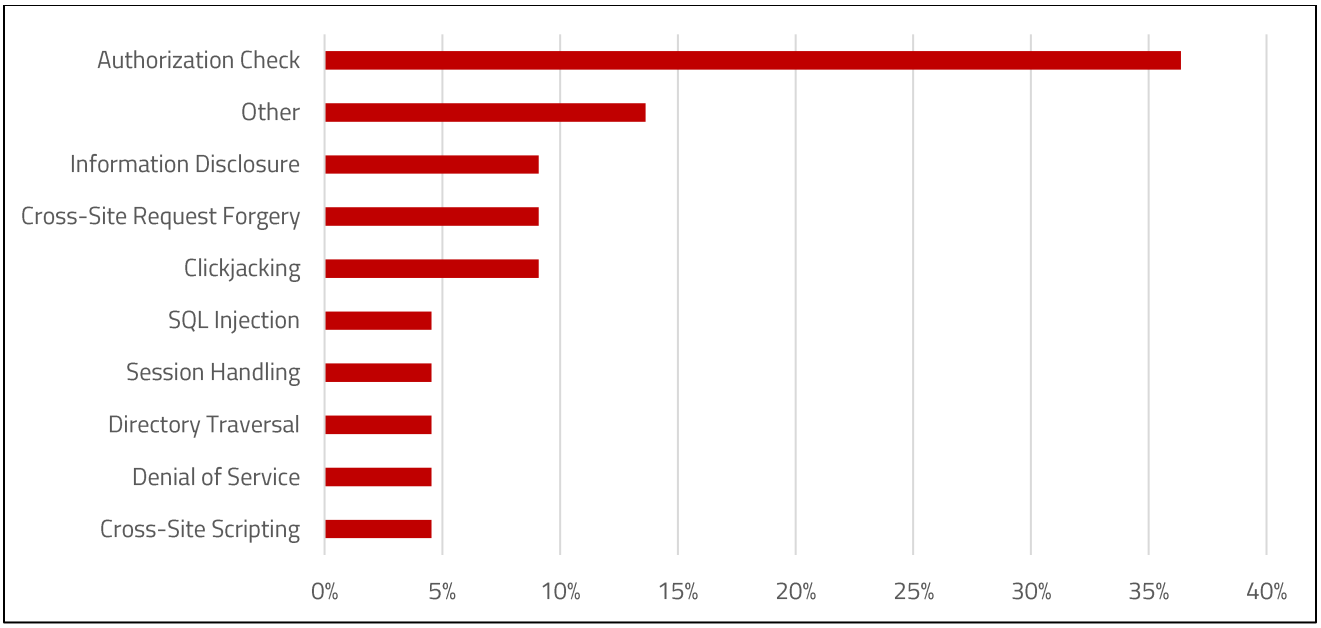
SAP Security Notes

September 2016

Note 1511193 deals with a high risk Cross-Site Request Forgery (XSRF) vulnerability in the CCMS Monitoring Console. XSRF is a common attack that exploits the trust relationship between applications and browsers, particularly stateful applications such as the CCMS Monitoring Console that use session cookies to group HTTP requests into a common session. XSRF attacks draw users to inadvertently click on URLs containing malicious or unauthorized requests. The requests often exploit the identity and privileges of the users to perform state-changing actions in an application. Attacks are also frequently used with cross-site scripting exploits to present malicious links to victims.

Applications are especially vulnerable to such attacks when users navigate to untrusted web sites using a browser that has a parallel session with an application server. XSRF vulnerabilities cannot be fully mitigated by techniques such as HTTPS or URL rewriting. Therefore, tokens containing complex cryptographic values are often used by servers to authenticate each user request.

Other high priority vulnerabilities patched in September include SQL injection and error checking flaws in Sybase ASE (Notes 2353243 and 2358986). Both vulnerabilities have high CVSS scores and can lead to the execution of arbitrary commands and stored procedures including SQL statements through the elevation of privileges. The impacted product version is ASE 16.0.



SAP Security Notes by Vulnerability Type

Notes 1627922 and 2318530 remove missing authentication checks in Basis and FI components including the function module SAA_REMOTE_OP_TRANSACTION used to perform operating system commands.

Note 2335687 extends SAP's whitelist based approach for protecting against clickjacking attacks to components of Customer Relationship Management (CRM).

Finally, Note 2172049 removes a Dynamic Link Libraries (DLL) hijacking vulnerability in SAP Financial Consolidation. DLLs are standalone files often used by EXEs in Windows systems. Since programs load DLLs at startup, DLL hijacking can lead to the execution of malware embedded in malicious DLLs installed by attackers.

Appendix: SAP Security Notes, September 2016 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	1511193	BC-CCM-MON	XSRF protection for the CCMS Monitoring Console
HIGH	2358986	BC-SYB-ASE	Insufficient error checking in SAP ASE
HIGH	2353243	BC-SYB-ASE	SQL Injection vulnerability in SAP ASE
HIGH	1627922	BC-SRV-NBC	Missing authorization check in SAA_REMOTE_OP_TRANSACTION
HIGH	2318530	XX-CSC-RU-FI	Missing authorization check in FI-LOC-SD-RU
MEDIUM	2029397	CRM-ISA-R3	Missing authorization checks for RFC in E-commerce ERP applications
MEDIUM	2251513	XX-PROJ-FI-CA	Missing authorization check in XX-PROJ-FI-CA
MEDIUM	2335687	CRM-SLC	Whitelist based Clickjacking Framing Protection in Solution Sales Configuration
MEDIUM	2316942	SCM-EWM-DLP	Missing Authorization check in EWM for delivery / warehouse request objects
MEDIUM	2181460	BC-XI-IBC	Unauthorized usage of application functionality in SAP Exchange Infrastructure
MEDIUM	2357695	CA-FIM-FCO	Missing Authorization check of Individual Conditions
MEDIUM	2353024	FS-AM-IM-IT	Missing Authorization check in Item Management
MEDIUM	2357856	CA-FIM-FCO	Missing Authorization check of Standard Conditions
MEDIUM	2350574	BC-SYB-ASE-CE	Address axis.jar security vulnerability (CVE-2014-3596) in SAP ASE Web Services component
MEDIUM	2292351	BI-BIP-LCM	Cross-Site Scripting (XSS) vulnerability in SAP BI Promotion Management Application

Appendix: SAP Security Notes, September 2016 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2347944	HAN-LM-INS-DB	Information disclosure in the CCMS agent of SAP HANA
MEDIUM	2290548	BI-BIP-INV	Denial of service (DOS) vulnerability in BI Launchpad
MEDIUM	2172049	EPM-BFC-TCL	Dll Hijacking in SAP Financial Consolidation
MEDIUM	2342473	BC-CCM-CNF-PFL	Directory Traversal vulnerability in Profile Maintenance
MEDIUM	2344524	BC-GP	Information Disclosure in Guided Procedures
MEDIUM	2351352	GRC-SAC-ARQ	The User Sessions were not handled correctly from End User Login Application.
MEDIUM	2319727	BC-SEC	Clickjacking protection framework in SAP NetWeaver AS ABAP and AS Java

LAYER SEVEN SECURITY

Layer Seven Security empowers organizations 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

1-555 Industrial Drive
Suite 107
Milton, Ontario
L9T 5E1, Canada

Web

www.layersevensecurity.com

Email

info@layersevensecurity.com

Telephone

1-647-964-7207