Layer Seven Security

ADVISORY

SAP Security Notes

August 2014

SAP Security Notes

August 2014

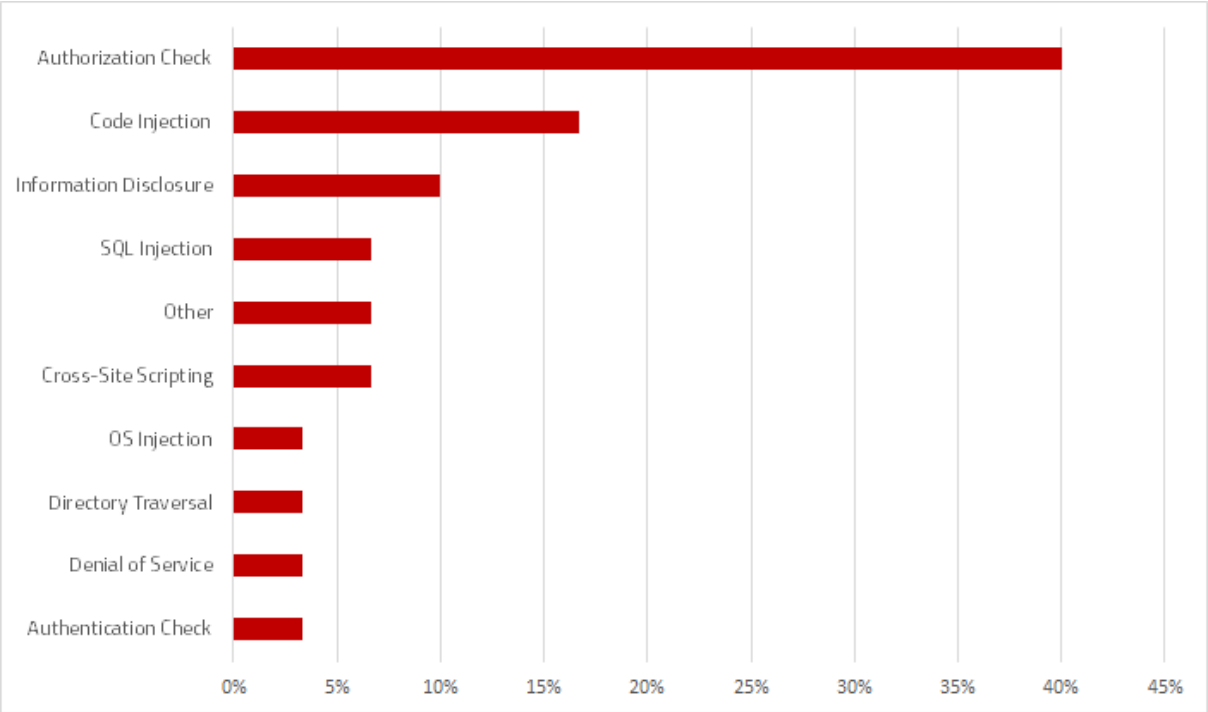
SAP released a Hot News fix in August for a critical vulnerability effecting the SAP Afaria Mobile Device Management (MDM) server. Note 2044175 patched security flaws in specific APIs supporting iOS device management that led to a failure to authenticate incoming devices. The vulnerability could be exploited to provoke a denial of service or control mobile devices remotely. Customers using Afaria 7SP4, 7SP3 are strongly recommended to apply Hotfix10 (7SP4AfariaFx10) and Hotfix40 (7SP3AfariaFx40) on the Afaria MDM Server.

Note 1917381 patched a missing authorization check that could be exploited to access a remote-enabled RFC function in Profile Maintenance The Note extends an authorization check for object S_RZL_ADM for the relevant function. The authorization object S_RZL_ADM supports system administration through the Computing Center Management System (CCMS).

Note 2025931 included a kernel patch to address a dangerous buffer overflow exploit. The vulnerability could lead systems to process malicious code injected into working memory but requires the ability to create and run new ABAP source code or modify existing code.

Note 1953562 addressed another critical code injection vulnerability that could enable attackers to, among other things, create privileged users and access, modify or delete sensitive data in Card Management. This is a component of Account Management in SAP Banking Services used to administer customer accounts including credit and other form of payment cards.

Finally, Note 1769064 introduced additional values for the auth/rfc_authority_check profile parameter and enables SAP system function modules to be defined with greater granularity. The parameter can be used to control access to system function modules such as RFC_SYSTEM_INFO which may be accessed



SAP Security Notes by Vulnerability Type

remotely and anonymously to obtain sensitive system information.

Appendix: SAP Security Notes, August 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2044175	MOB-AFA	CPR: Missing Authentication Controls on Afaria Server
HIGH	1917381	BC-CCM-CNF-PFL	Missing authorization check in Profile Maintenance
HIGH	1739143	BC-TRX-API	Possible OS command injection on TREX/BWA server
HIGH	2025931	BC-SEC	Potential remote code execution in BC-SEC
HIGH	2026174	BI-BIP-INV	SBOP solution for Apache Struts1.x Vulnerability CVE-2014-0094
HIGH	2028484	HAN-DB	Missing authorization check in SQL processing in HANA
HIGH	2030937	IS-B-BCA	Missing authorization check in IS-B-BCA
HIGH	2033789	IS-B-BCA-AM	Missing authorization check in IS-B-BCA
HIGH	2034140	BC-DWB-CEX-BAD	Missing authorization check in BAdI Activation
HIGH	2035964	IS-R-TRN-TFT	Potential information disclosure relating to NFM from TPS Systems, Inc.
HIGH	2044220	BC-SYB-ASE	Missing authorization check and potential remote code execution in SAP ASE
HIGH	2053074	MOB-AFA	Potential modification of persisted data in Afaria Server
HIGH	1953562	FS-AM-CM-CA	Code injection vulnerability in Card Management
HIGH	1870485	CA-EUR	Missing authorization check in CA-EUR
HIGH	1987773	XX-CSC-AR-FICA	Directory traversal in XX-CSC-AR-FICA
HIGH	1988496	IS-B-BCA	Missing authorization check in IS-B-BCA
HIGH	1992114	SV-SMG-TWB-BCA	Missing authorization check in SV-SMG-TWB-BCA
HIGH	2003859	SRM-EBP-SHP	Missing authorization check in SRM Shopping cart
HIGH	2017651	SRM-CAT-MDM	Potential information disclosure relating to SRM-EBP-CAT
HIGH	2018221	BC-ABA-SC	Bufferoverflow in ABAP VM
HIGH	2020395	BC-INS-FWK	Sapinst used static salt for password encryption on UNIX / Linux
HIGH	2021253	IS-B-BCA	Missing authorization check in IS-B-BCA
HIGH	2021376	MOB-AFA	Potential denial of service in Afaria Server
HIGH	2024272	IS-B-BCA-AM	Missing authorization check in IS-B-BCA-AM

Appendix: SAP Security Notes, August 2014

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2032840	BC-CST	Potential information disclosure relating to BC-CST
MEDIUM	2033775	MOB-AFA	Potential modif./disclosure of persisted data in Afaria
MEDIUM	1997266	EP-PIN-NAV	Unauthorized modification of stored content in Portal Masthead
MEDIUM	1999142	BI-RA-CR	Potential remote code execution in BI-RA-CR
MEDIUM	1769064	BC-MID-RFC	Additional values for auth/rfc_authority_check
MEDIUM	2012215	BI-BIP-INV	Unauthorized modification of displayed content in BI-BIP-INV

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