Layer Seven Security

ADVISORY

SAP Security Notes

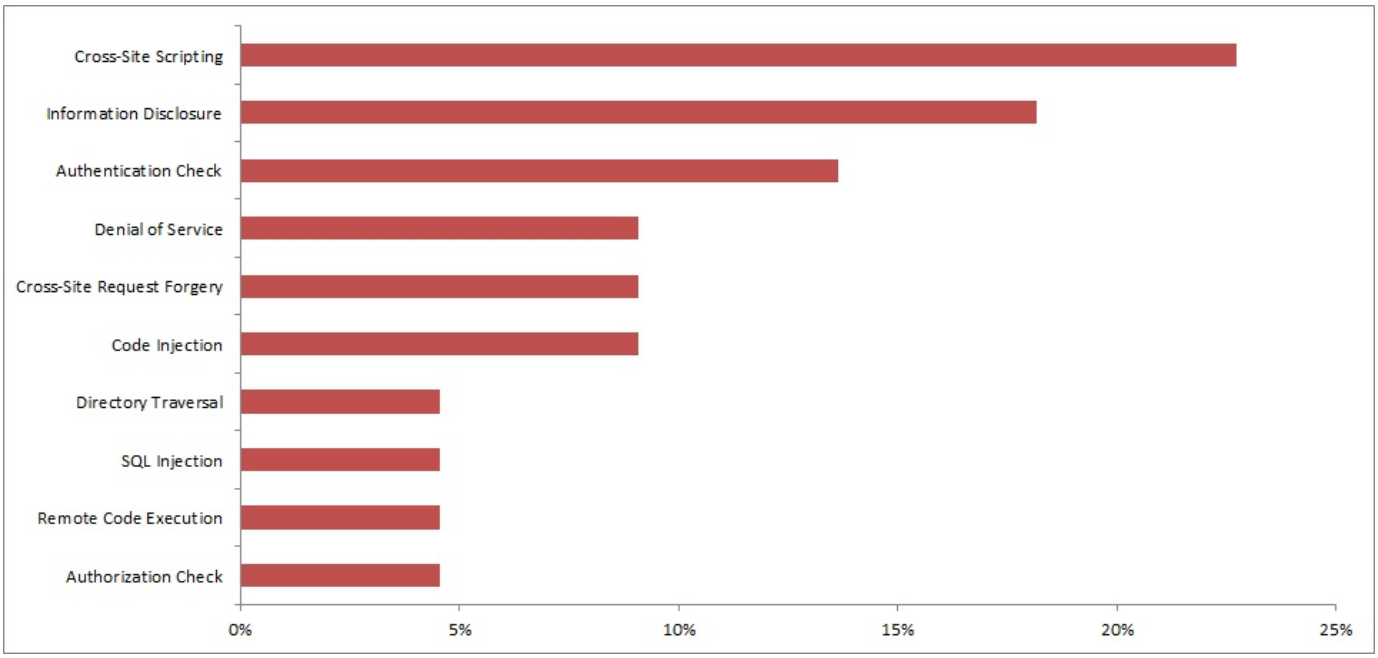
June 2014

SAP Security Notes

June 2014

SAP released an important notification in June to highlight a critical vulnerability in SAP Afaria, the Sybase platform that enables centralized control of mobile iOS, Android, BlackBerry and Windows devices. Afaria can be deployed on premise or leveraged through cloud-based partners. It enables organizations to secure both corporate and personal devices through the application of flexible, scalable security policies. Note 2028012 deals with a vulnerability in the Afaria mobile app that could lead to the discovery of user credentials transmitted to servers during device enrolment. The vulnerability does not impact all landscape scenarios but is nonetheless rated as critical by SAP. iOS and Android users are advised to update their apps to versions 6.60.6417.1 and 6.60.6417, respectively, available through the Apple Store, Google Play, and the SAP portals for Afaria and Mobile Secure Cloud. Customers are also advised to change active directory credentials and implement the related hotfix for the SAP Afaria server. The latter will prevent the enrolment of new devices that have not been updated to the latest versions of the Afaria mobile app.

SAP also introduced changes for improved session protection in the BusinessObjects Business Intelligence (BI) platform. In common with other Java EE applications, BI uses system cookies to track session-related data including logon information. This information could be exposed through client side scripts using techniques such as cross-site scripting. Enabling the HttpOnly attribute removes this risk by disabling access to system cookies from client-side scripts, applets and plugins. However, this often impacts the performance of applets and other functions that require access to authentication information in cookies. Enabling the HttpOnly flag in BI 4.0, for example, impacts the function of the Webi Intelligence Java viewer. According to Note 1981048, customers can resolve this issue by using version JRE7 after upgrading to BI 4.1 which includes Tomcat version 7 with



SAP Security Notes by Vulnerability Type

HttpOnly enabled by default. Customers can also manually change their existing Tomcat configurations to enable improved session protection.

Note 2007530 contains instructions for using shadow passwords in UNIX systems with the SAP Content Server. The use of shadow passwords is highly recommend since it can be used to restrict access to sensitive OS-level password files to privileged root users. Unprivileged users are therefore unable to access password hashes stored in files to perform brute force or dictionary attacks. Unix distributions that do not use shadow passwords store encoded passwords in the world readable /etc/passwd file.

Lastly, SAP released several Notes for vulnerabilities in the browser based developed tool for SAP HANA known as the Web-based Development Workbench. This includes patches for code and SQL injection vulnerabilities through Notes 2015446 and 2014881, effecting specific versions.

Appendix: SAP Security Notes, June 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2028012	MOB-AFA	Vulnerability in Afaria mobile device app
HIGH	1881073	BC-CST	Unauthorized modification of displayed content in BSP application
HIGH	1908531	BI-RA-EXP	Untrusted XML input parsing possible in SBOP Explorer
HIGH	1941562	BI-BIP-INV	Unauthorized modification of stored content in BI-BIP-INV
HIGH	1943208	EP-KM-CM	Unauthorized modification of stored content in KM Content Management
HIGH	1967780	BW-WHM-DST	Missing authorization check in BW-WHM-DST
HIGH	1971270	BI-BIP-INV	Unauthorized modification of displayed content in BI-BIP-INV, BI-BIP-QB, BI-BIP-BIW
HIGH	1981048	BI-BIP-INV	HTTP Cookies Without HttpOnly Flag Set may lead to Cross Site Scripting Issues
HIGH	1998990	BI-BIP-ADM	Potential information disclosure relating to BI-BIP-ADM
HIGH	2001106	BI-BIP-ADM	Potential denial of service in BI-BIP
HIGH	2001109	BI-BIP-AUT	Potential information disclosure relating to BI-BIP-AUT
HIGH	2006974	PP-PI-CFB	Code injection vulnerability in PP-PI-CFB
HIGH	2007526	BC-SRV-KPR-CS	Potential information disclosure relating to BC-SRV-KPR-CS
HIGH	2007530	BC-SRV-KPR-CS	Invalid User Authentication in Unix SAP Content Server
HIGH	2014881	HAN-WDE	Potential disclosure of persisted data in SAP HANA Web-based Development Workbench
HIGH	2015446	HAN-WDE	Unauthorized use of application functions in SAP HANA Web-based Development Workbench via code injection
HIGH	2026132	BC-MID-ICF-LGN	Update 1 to security note 1483548
HIGH	2028891	BC-SYB-ESP	Remote Code Execution Vulnerability in Sybase ESP 5.1
MEDIUM	1962860	EPM-BPC-NW	Unauthorized use of application functions in BPC 7.5
MEDIUM	2026971	PP-PI-CFB	Flaw in SMP Android Object API libraries
MEDIUM	2028916	BI-BIP-ADM	Flaw in SMP Android Object API libraries
MEDIUM	2032811	MOB-SUP-SDK	Directory traversal in PY-PH

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