Layer Seven Security

ADVISORY

SAP Security Notes

November 2012

SAP Security Notes

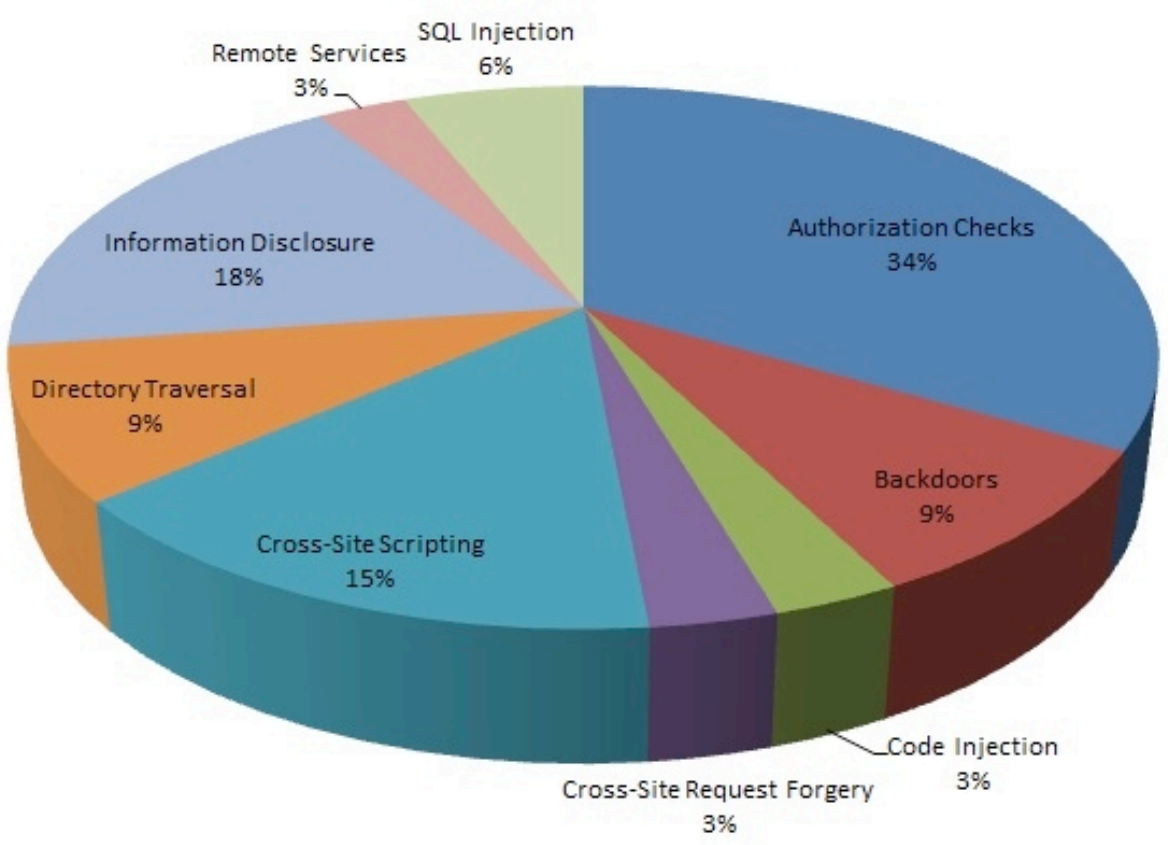
November 2012

In February 2012, SAP released a critical Security Note that advised customers to delete the AUTOMATION_ALV function group which included a dangerous automated BAPI routine that was delivered only for test purposes. BAPIs are SAP application programming interfaces used for inbound and outbound processing. Note 1597597 recommended the deletion of the AUTOMATION_ALV using SE80. In November, SAP issued revised instructions in Note 1715002, including a deletion transport for the function group. Customers are strongly advised to implement the transport if the function was manually deleted in line with the directions provided in the earlier Note.

Customers should also closely review Note 1682613 which carries a CVSS base score of 10. SAP rarely assigns such a high rating to Security Notes. This specific Note deals with unauthenticated access to file service functions in the core runtime environment of the J2EE engine. The vulnerability can lead to an escalation of privileges in a vital area of the NetWeaver AS Java.

Note 1749068 also deals with an escalation of privileges vulnerability, this time related to the Treasury and Risk Management (TRM) component of SAP Financial Supply Chain Management (FIN-FSCM). FIN-FSCM is used to optimize the flow of financial and other information within organizations and between business partners. The vulnerability affects account management functions in the Transaction Manager used to manage financial transactions and positions and perform liquidity and risk analysis.

SAP released an unusually high number of Security Notes in November to remove hard-coded credentials that provide potential backdoor access to a variety of applications. This includes the External Data Transfer (EDT) component of SAP Banking (Note 1753036), the ABAP Class Builder, used to maintain the ABAP class library (Note 1768068) and SAP Mobile Infrastructure (Note 1579478).



SAP Security Notes by Vulnerability Type

SAP Mobile Infrastructure (BC-MOB-MI-SER) also suffered from SQL injection and information disclosure vulnerabilities, patched through Notes 1579948 and 1580088 in November.

Another SAP area patched in November for SQL injection vulnerabilities was the STR component of SAP Retail (IS-R) used to replace standard texts with retail-specific texts (refer to Note 1673713).

SAP also released a patch for an injection flaw in the Computing Center Management System (CCMS) alert monitor. This is used to trigger alerts to System Administrators for performance values that exceed predefined thresholds in areas such as background processing, load balancing, scheduled backups and system availability. Note 1758450 includes a set of files and executables to prevent users from injecting and running their own code, modifying and deleting data, creating new users with escalated privileges, and performing other undesirable actions.

Appendix: SAP Security Notes, November 2012

PRIORITY	NOTE	AREA	DESCRIPTION
1	1715002	BC-SRV-ALV	Update 1 to security note 1597597
1	1682613	BC-JAS-COR	Missing authorization check in core service
2	1775705	EP-PIN-PRT	Update 2 to Security Note 1630293
2	1711728	BC-XI-IBD-MAP	Removal of Hidden menus and Developer mode in ESR
2	1715040	BC-CCM-MON	Potential information disclosure relating to arbitrary file
2	1734398	BC-JAS-ADM-MON	Potential information disclosure relating to AS Java
2	1734986	BC-CST-STS	Unauthorized usage of functions in SAP start service
2	1736663	PA-TM	Missing authorization check in PA-TM
2	1737798	CRM-ISA-BCS	Unauthorized modification of displayed content in CRM-ISA-BC
2	1749068	FIN-FSCM-TRM-TM	Missing authorization check in security account management
2	1750920	FS-AM-CM-CF	Missing authorization check in FS-AM-CM-CF
2	1753036	IS-B-DP-EDT	Hard-coded credentials in IS-B-DP-EDT
2	1755530	IS-B-DP-EDT	Directory traversal in IS-B-DP-EDT for report SAPLKXDM
2	1768068	BC-DWB-TOO-CLA	Hard-coded credentials in ABAP Class Builder
2	1774568	SV-SMG-DIA-SRV-AGT	Disable (RSC) service exposed by the Diagnostics Agent
2	1697254	CA-GTF-RCM	Unauthorized modification of displayed content in CA-GTF-RCM
2	1553180	BC-CST-DP	Missing authorization check
2	1579478	BC-MOB-MI-SER	Hard-coded credentials in BC-MOB-MI-SER
2	1579948	BC-MOB-MI-SER	Potential modification of persisted data in BC-MOB-MI_SER
2	1580088	BC-MOB-MI-SER	Potential disclosure of persisted data in BC-MOB-MI-SER
2	1591517	CRM-BF-CFG	Directory traversal in CRM IPC
2	1626650	XAP-EM	Cross site scripting adaption of EC 30 pivot query HTML view
2	1637408	IS-R-RA	Potential modification or disclosure of persisted data in RA
2	1641379	BC-SRV-KPR-CMS	Potential disclosure of persisted data in BC-SRV-KPR
2	1662930	PA-CP	Unauth. modification of displayed content in Detail Planning
2	1673713	IS-R-STR	Potential modification of persisted data in IS-R-STR

PRIORITY	NOTE	AREA	DESCRIPTION
2	1679897	BC-XI-CON-AFW	PI SEC: Potential information disclosure in PI AF
2	1686172	IS-B-DP-EDT	Missing authorization check in IS-B-DP-EDT
2	1758450	BC-CCM-MON	Code injection vulnerability in CCMS Agent
3	1772190	CA-WUI	Unauthorized use of application functions in WEBCUIF
3	1597598	BC-MID-ICF	Missing authorization check in ICF
3	1652271	BC-SRV-ADR	Missing authorization check in BC-SRV-ADR
4	1486584	CRM-MD-PRO	Unauthorized modification in BSP application CRM_PRD_TEST_UI

Layer Seven Security

Layer Seven Security specialize in SAP security. We serve customers worldwide to protect information assets against internal and external threats and comply with industry and statutory reporting requirements. The company fuses technical expertise with business acumen to deliver unparalleled implementation, consulting and audit services targeted at managing risks in contemporary SAP systems.

Layer Seven Security leverage leading SAP-certified software to deliver end-to-end assessments that detect and remediate vulnerabilities at all levels in SAP landscapes.

The company is privately owned and headquartered in Toronto, Canada.

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