ADVISORY

Layer Seven Security

SAP Security Notes

July 2013

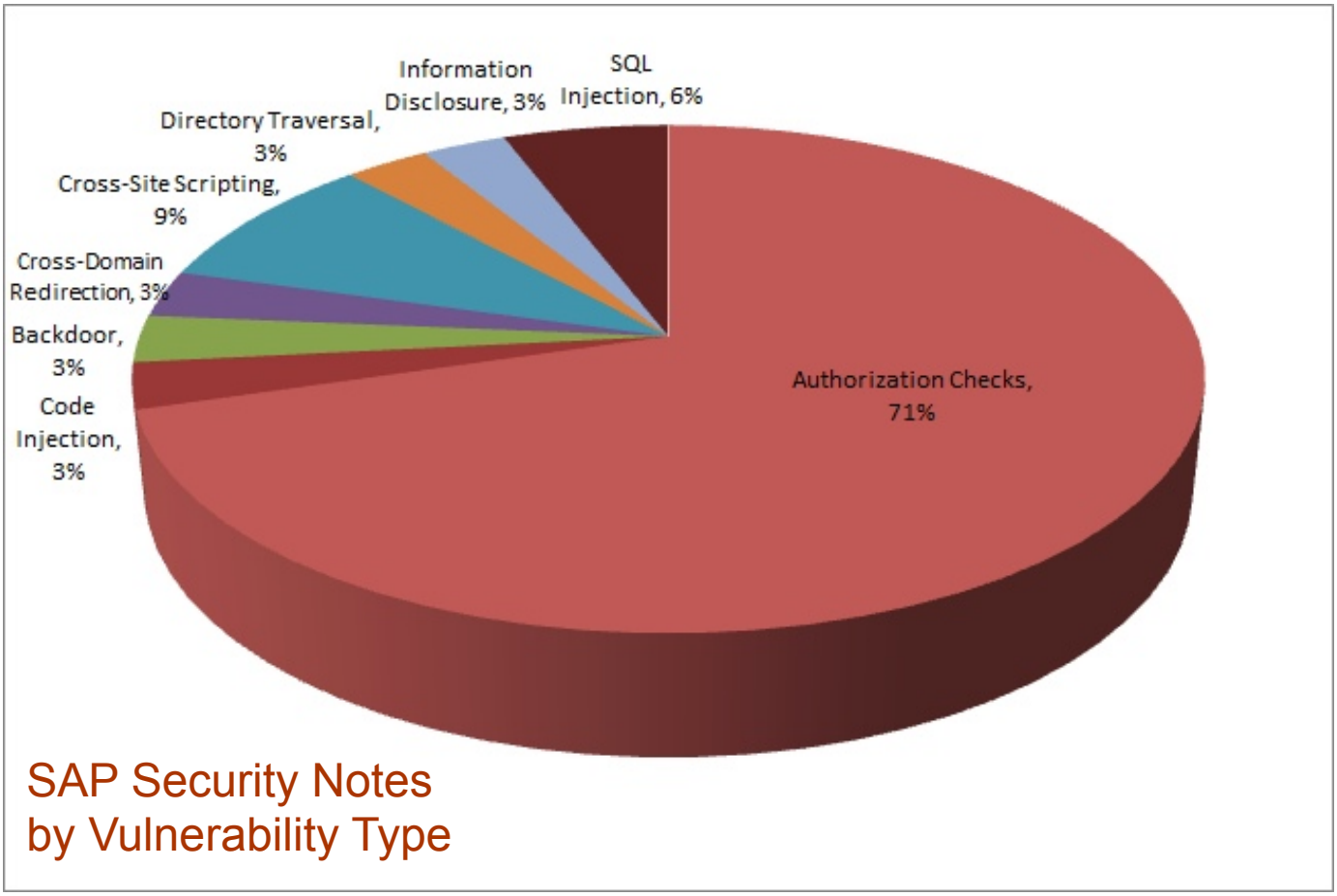
SAP Security Notes

July 2013

Patches for missing authorization checks typically account for the majority of SAP Security Notes in any given month. Such checks are enabled at multiple levels including transaction code, program, function module and table level in order to ensure that users have the appropriate permissions to perform actions in SAP systems. Given the complexity and volume of transactions, programs, etc. across all applications and components, it's not unusual for some expected checks to be absent in standard functions. Therefore, SAP works diligently with customers to identify and repair missing checks through Security Notes. Nonetheless, the number of Notes released by SAP that dealt specifically with missing authorization checks was abnormally high in July. In all, SAP issued 24 notes to address missing checks, which accounted for over 70 percent of all Notes released last month.

The most significant Notes dealt with missing checks in components of the SAP Account Management system (FS AM) that enable users to manage payment conditions for loans and other contractual arrangements between business partners and banks (Notes 1859165 and 1850704), as well as areas of Contract Accounts Receivable and Payable (FI-CA) that integrate directly with SAP Credit Management (Note 1851835). Other Notes patched missing authorization checks in the eAccounting engine of Financials (1853756), product master data management in the SAP industry solution for media (1853040) and Process Management (PP-PI-PMA) in Production Planning (1864397). The latter impacts execution steps in process management. PP-PI-PMA is used by manufacturing companies for data exchange with industrial control systems, quality management, inventory management, batch production and plant maintenance.

Note 1870605 deals with a programming flaw in the source code of the SAP Hana database that could be exploited to escalate privileges to a system-wide level without



SAP Security Notes by Vulnerability Type

authorization. As a result, customers are advised to update to at least revision 57 of SAP Hana.

A correction for the Internet Sales Application (ISA) of SAP CRM was released through Note 1861295 for a reflected cross-site scripting vulnerability caused by insufficient encoding of OUTPUT parameters by pages within ISA. The vulnerability could lead to the theft of user credentials including credentials for Administrators which could compromise the security of the entire application.

Note 1881391 relates to a code injection vulnerability affecting the XML for Analysis (XMLA) interface in Business Warehouse.

The Note recommends deactivating the XLMA service in the Internet Communication Framework if it is not in use. XLMA is less frequently used than alternative interfaces such as OLAP BAPI and OLE DB for OLAP. Therefore, deactivation should be possible in the majority of cases.

Appendix: SAP Security Notes, July 2013

PRIORITY	NOTE	AREA	DESCRIPTION
2	1885280	BC-SRV-GBT-ALM	Update 1 to security note 1610668
2	1854252	BC-SRV-ALV	Missing authorization-check in BC-SRV-ALV
2	1856093	CA-MRS	Missing authorization check in CA-MRS
2	1858474	PM-EQM-SF-MPC	Missing authorization check in PM-EQM-SF-MPC
2	1858566	FIN-FSCM-TRM-TM	Missing authorization check in Market Data Upload
2	1859165	FS-AM-CM-AC	Missing authorization check in Inpayment agreement, BCDP
2	1860278	EC-CS	Missing whitelist check in FI-LC, EC-CS, and EC-EIS
2	1860367	CO-PA	Missing authorization check in CO-PA
2	1861295	CRM-ISA	Unauthorized modification of displayed content in CRM-ISA
2	1863091	ICM-TO	Missing authorization check in ICM
2	1863150	BC-ABA-SC	Missing authorization check in BC-ABA-SC
2	1864397	PP-PI-PMA	Missing authorization check in Process Management.
2	1868012	PY-CH	Missing whitelist check in PY-CH
2	1870605	BC-DB-HDB	Privilege escalation in SAP HANA
2	1881391	BW-BEX-OT-MDX	MDX: XML for Analysis - known security holes
2	1808106	BC-SRV-COM-FTP	Update #2 to Security Note 1692988
2	1839699	CA-MRS	Missing authorization check in CA-MRS
2	1840304	PSM-EC	Missing authorization check in Expenditure Certification
2	1846515	BC-SRV-REP	Missing authorization check in BC-SRV-REP
2	1846653	BC-DB-LCA-DP	Remote Arbitrary Program Excn in LCAPPS DP
2	1850704	FS-AM-CM-AC	Missing authorization check in agreement(BCDL) FS-AM-CM-AC
2	1851835	XX-PROJ-FI-CA	Missing authorization check in FI-CA
2	1852738	PA-PA-ZA	Missing authorization check in PA-PA-ZA
2	1853040	IS-M-MD-PR	Missing authorization check in IS-M
2	1853756	FIN-BAC-AE	Missing authorization check in eAccounting

Appendix: SAP Security Notes, July 2013 cont.

PRIORITY	NOTE	AREA	DESCRIPTION
3	1876993	CA-UI2-INT-BE	UI2: missing authorization check when adding a Chip
3	1857350	BI-BIP-BIW	Unauthorized modification of displayed content in BIW
3	1798286	SCM-BAS-EHS	Potential modif./disclosure of persisted data in SCM
3	1819984	BC-JAS-COR	Potential illegal redirection of Web site content in AS Java
3	1823687	BC-SEC-LGN	Potential information disclosure relating to user existence
3	1831022	BC-CTS-CMS	Missing Authorization Check in DI_CMS (BC-CTS-CMS)
3	1831053	BC-CTS-CMS	Missing Authorization Check in CM Services (BC-CTS-CMS)
3	1833327	BC-SRV-ADR	Potential disclosure of persisted data in BC-SRV-ADR
3	1833485	BI-BIP-BIW	Unauthorized modification of displayed content in BIW

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