ADVISORY

Layer Seven Security

SAP Security Notes

August 2013

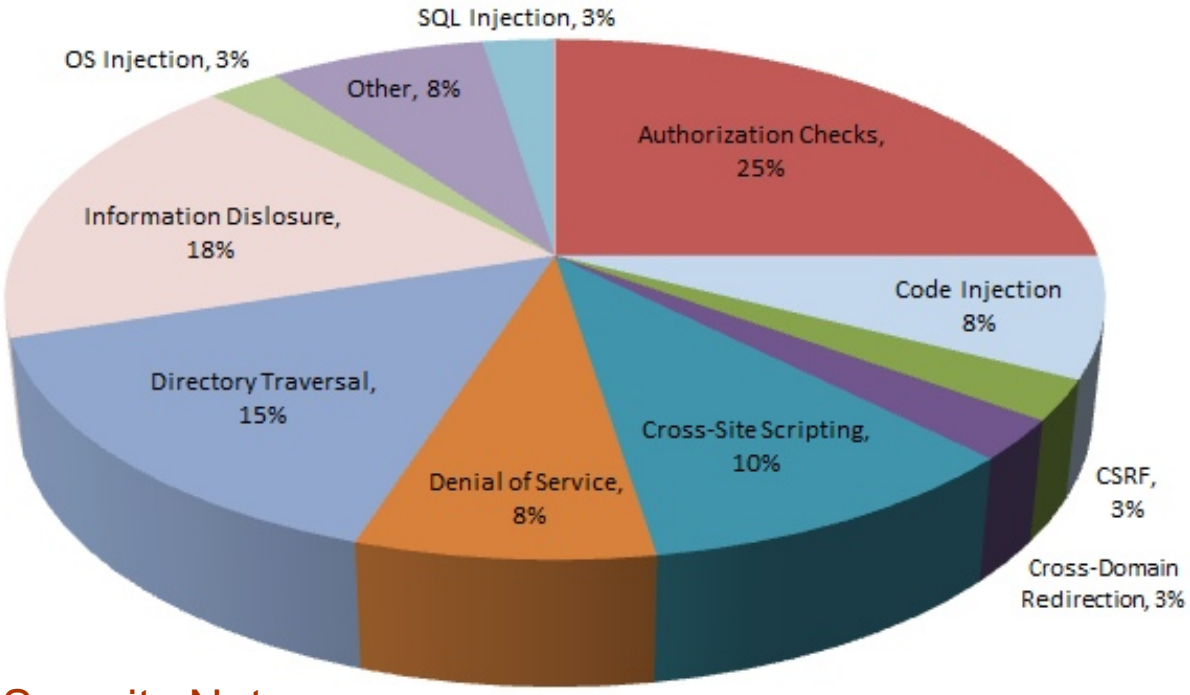
SAP Security Notes

August 2013

One of the most important patches released by SAP in August related to a vulnerability in the Solution Tools Plug-in (ST-PI) that enables users to execute arbitrary OS commands (Note 1861791). ST-PI supports data collection and is installed on every system in SAP landscapes. The vulnerability affects the Service Data Download component (SV-SMG-SDD) that was patched for a similar vulnerability in February 2012 via Note 1641329. External commands including commands directed at SAP hosts should be performed through SXPG_CALL_SYSTEM or SXPG_COMMAND_EXECUTE. These function modules check for the appropriate user authorizations before executing commands. OS commands are registered through transaction SM69 and run through SM49. Unauthorized OS commands can lead to the complete compromise of SAP systems.

Arbitrary ABAP commands are equally dangerous. This occurs when externally-provided user input is not adequately validated by dynamically generated SAP programs or reports. Such commands can alter the execution of SAP processes, inject backdoors or rootkits in programs and lead to malicious changes to SAP data. Note 1873131 patched an ABAP code injection vulnerability in the Stock Inconsistencies component of MM-IM used to control physical inventories in Materials Management.

The support package included in Note 1880040 resolved a resource exhaustion condition in the Sybase SQL Anywhere server that could be exploited to provoke a denial of service. SQL Anywhere is widely used as an embedded database in enterprise and mobile applications. Resource exhaustion vulnerabilities are notoriously difficult to guard against since common solutions for the vulnerability may block access for system or end users if attackers impersonate a legitimate user or simply increase the number of simultaneous



SAP Security Notes by Vulnerability Type

requests required to exhaust system resources.

SAP released multiple Notes to address directory traversal vulnerabilities affecting Business Intelligence (Note 1867210), CRM (1874456 and 1875158), AS Java (1753378), ERP Sales and Distribution (1781994) and Mobile components (1796761). Directory traversal is one of the most common vulnerabilities in ABAP programs. A familiar variation of directory traversal attacks involves altering backslash and forward-slash character sequences in URLs for resource locations. ABAP programs use commands such as OPEN DATASET to access files stored in application servers. Some programs enable users to specify file names through selection screens or other interfaces. Insufficient validation of user input could enable attackers to access restricted or sensitive files on application servers without authorization. Such attacks can be countered through the proper use of the FILE_VALIDATE_NAME function module which validates physical file names against a whitelist of logical file names. The whitelist is maintained in customizing tables accessible through transaction SFIL or the path *IMG – Application Server – System Administration – Logical File Names.*

Appendix: SAP Security Notes, August 2013

PRIORITY	NOTE	AREA	DESCRIPTION
2	1845802	EHS-SAF-RCK	Missing authorization check in EHS-SAF-RCK
2	1847217	BW-BEX-OT	Missing authorization check in BW-BEX-OT
2	1847811	BC-CST-IC	Potential information disclosure relating to SMICM
2	1851123	BC-BSP	Potential false redirection of Web site content in BSP
2	1852955	PP-BD-RTG	Privilege Escalation in PP-BD-RTG
2	1856296	CA-LT-CNV	Missing authorization check in CA-LT-CNV
2	1860308	CA-GTF-MDC	Missing authorization check in CA-GTF
2	1861791	SV-SMG-SDD	OS CMD injection vulnerability in ST-PI
2	1863815	BW-BEX-OT-OLAP	Missing authorization check in BW-BEX-OT-OLAP
2	1865302	CO-PA	Code injection vulnerability in CO-PA
2	1873131	MM-IM-GF-INC	Code injection vulnerability in MM-IM
2	1880040	BC-SYB-SQA	Potential denial of service in SQL Anywhere
2	1611963	FIN-SEM-CPM	Update #1 to Security Note 1509929
2	1688229	SV-SMG-SDD	Information disclosure due to missing auth. in EWA functions
2	1765099	CRM-MKT-MPL-ST-PRO	Missing authorization check in CRM-MKT-MPL-ST-PRO
2	1772529	BC-ILM-LCM	Missing authoriztion check in BC-ILM-LCM
2	1773651	BW-BEX-UDI	Potential disclosure of persisted data in BW-BEX-UDI-SDK
2	1804016	EHS-MGM-INC	Potential information disclosure in incident management
2	1835125	BC-ESI-WS-JAV-RT	Untrusted XML input parsing possible in sapxmltoolkit
2	1838451	EP-KM-CM	Untrusted XML input parsing possible in Pipeline Service
3	1864081	FIN-FSCM-TRM-TM-TR	Missing Authorization Check in TRM Transaction Management
3	1866659	WEC-APP-BF	XSS Hardening of attachment downoload
3	1867210	BI-RA-CR	Directory traversal in BI-RA-CR
3	1867641	CRM-CIC	Unauthorized modification of displayed content in CRM-CIC
3	1870426	CRM-RPL-SRV-RPT	Code injection vulnerability in CRM-RPL-SRV-RPT

Appendix: SAP Security Notes, August 2013 cont.

PRIORITY	NOTE	AREA	DESCRIPTION
3	1874456	CRM-BF-IIA	Directory traversal in CRM-BF-IIA
3	1875158	CRM-MD-SDB	Directory traversal in CRM-MD-SDB
3	1881221	BC-MID-BUS	HTTP Response Splitting in the SAP BC
3	1699357	CA-GTF-IC-CHA	Connection to Virus Scan Interface in CA-GTF-IC-CHA
3	1748268	SRM-EBP-CAT	Unauthorized modification of stored content in SRM-EBP-CAT
3	1753378	BC-JAS-WEB	Directory traversal in Web Container
3	1764298	BC-DB-SDB	Potential information disclosure relating to Database Studio
3	1772839	BC-SRV-ADR	Potential disclosure of persisted data in BC-SRV-ADR
3	1781994	SD-SLS	Directory traversal in SD-SLS
3	1796761	XAP-MBA-MSE	Directory traversal in CRM Handheld Service
3	1802680	EHS-MGM-INC	Potential information disclosure in incident tasks
3	1809965	BC-JAS-SEC	Unauthorized modification of displayed content in Logon App
3	1815105	BC-JAS-ADM-LOG	Missing authorization check in LogViewer
3	1840249	FIN-FB-SRV	Potential modif./disclosure of persisted data in ABAD0
3	1842817	BC-UPG-TLS-TLJ	Removal of encrypted data after an update/upgrade process

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