Layer Seven Security

ADVISORY

SAP Security Notes

March 2014

SAP Security Notes

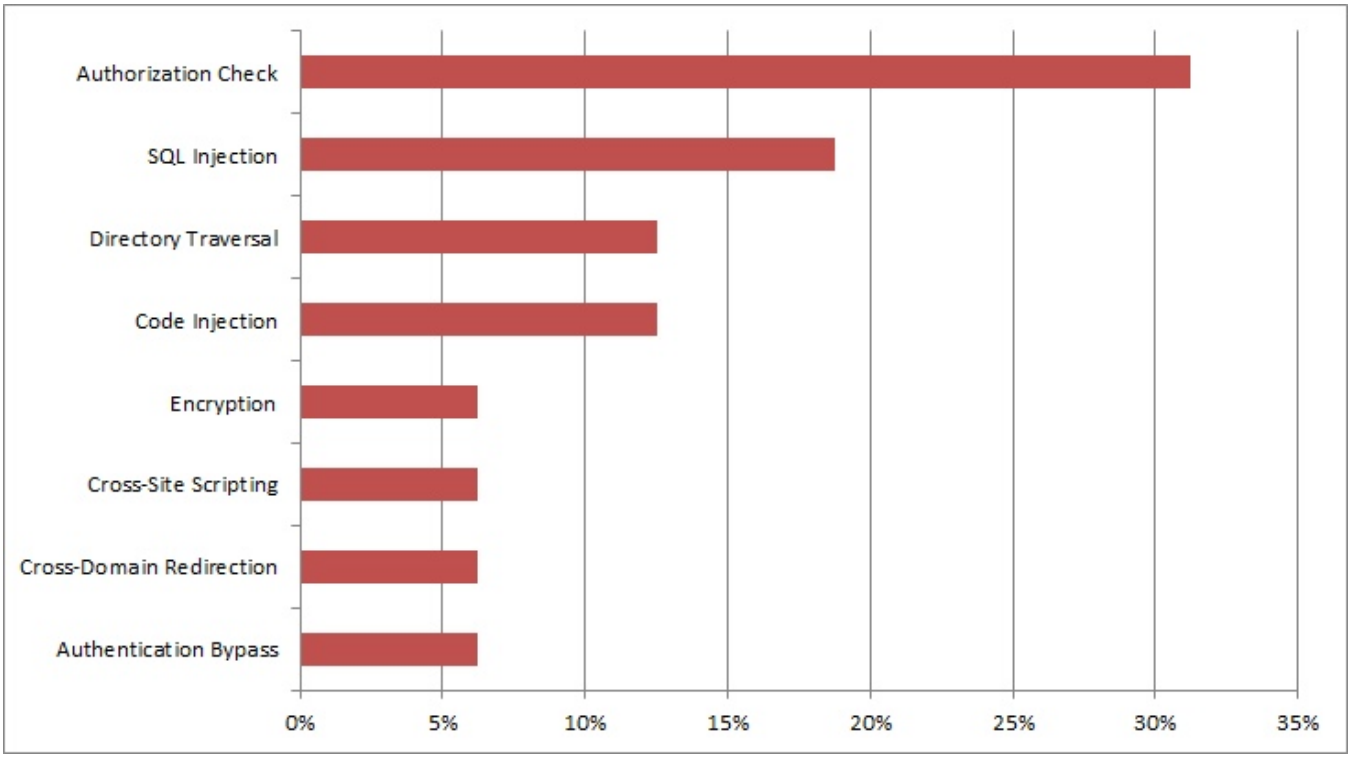
March 2014

The most significant Security Note released in March patched a crucial OS command vulnerability in SAP background processing used to automate routine and often resource-intensive tasks. Background processing provides a range of tools to schedule and manage jobs. It also supports external commands to enable processing steps outside SAP systems. This is performed using the SAP control program sapxpg through RFC.

There is a distinction between external programs and external commands. The former is performed by system administrators and is not subject to SAP authorization checks. External programs are therefore unrestricted commands. External commands, on the other hand, can be controlled using the SAP authorization concept. They can also be restricted to specific operating systems. This ensures that end users can only run authorized commands within particular external systems. External commands are maintained using transaction SM59 and can be run in CCMS using SM49. The authorization checks are performed via function modules such as SXPG_CALL_SYSTEM, SXPG_COMMAND_CHECK and SXPG_COMMAND_EXECUTE.

Note 1965610 contains corrections for a vulnerability in external commands that could enable attackers to inject arbitrary code to obtain sensitive information, corrupt data, escalate privileges or perform a denial of service. The Note introduces more stringent checks for additional parameters provided by end users.

Note 1966056 deals with a similar code injection vulnerability in the OLAP engine of Business Warehouse that drives decision support systems used for data modeling.



SAP Security Notes by Vulnerability Type

Note 1964428 patches an authentication flaw in SAP HANA Extended Application Services (XS) which integrates servers and development environments into HANA databases. The Note enables customers to effectively change access settings for applications that are configured for public access. Prior to the release of the Note, customers were unable to enforce changes to the authentication type for publically-accessible applications.

Note 1987210 targets a stored cross-site scripting vulnerability in the data source framework of the Payroll Control Center in Human Capital Management (HCM). The framework manages the logic and structure of on-screen check data displayed to users. The vulnerability could lead to the theft of authentication information for authorised users and administrators.

Finally, Note 1884678 provides detailed instructions for removing a vulnerability in Business Process Change Analyzer (BPCA) that could enable attackers to read files containing sensitive information through path traversal. BPCA is used to identify the specific objects impacted by transport requests in order to develop focused and streamlined test plans.

Appendix: SAP Security Notes, March 2014

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	1971238	BC-CUS-TOL-HMT	Missing authorization check in BC-CUS-TOL-HMT
HIGH	1966896	BW-BEX-OT	Missing authorization check in BW-BEX-OT
HIGH	1966056	BW-BEX-OT	Code injection vulnerability in BW
HIGH	1965610	BC-CCM-BTC	Code injection vulnerability in external commands
HIGH	1964428	HAN-AS-XS	XS bypasses authentication for former public applications
HIGH	1963564	IS-B-BCA-MD	Missing authorization check in IS-B-BCA
HIGH	1946420	SRM-LA	Potential false redirection of Web site content in SRM-LA
MEDIUM	1990096	CA-GTF-TS-GMA	Update 1 to security note 1644043
MEDIUM	1772839	BC-SRV-ADR	Potential disclosure of persisted data in BC-SRV-ADR
MEDIUM	1884678	SV-SMG-TWB-BCA	Potential directory traversals in BPCA
MEDIUM	1963932	HAN-AS-XS	Missing encryption for form based authentication
MEDIUM	1786150	CRM-MD-BP	Potential disclosure of persisted data in [crm-md-bp]
MEDIUM	1867167	CRM-IC-EMS-CAT	Potential modif./disclosure of persisted data,CRM-IC-EMS-CAT
MEDIUM	1837735	ICM-MD	Directory traversal in component ICM
MEDIUM	1987210	PY-XX-RS	Unauthorized modification of stored content in Payroll Data Source Framework
LOW	1955908	BC-BMT-WFM	Fehlende BerechtigungsprÃ¼fung in BC-BMT-WFM

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