ADVISORY

Layer Seven Security

SAP Security Notes

October 2013

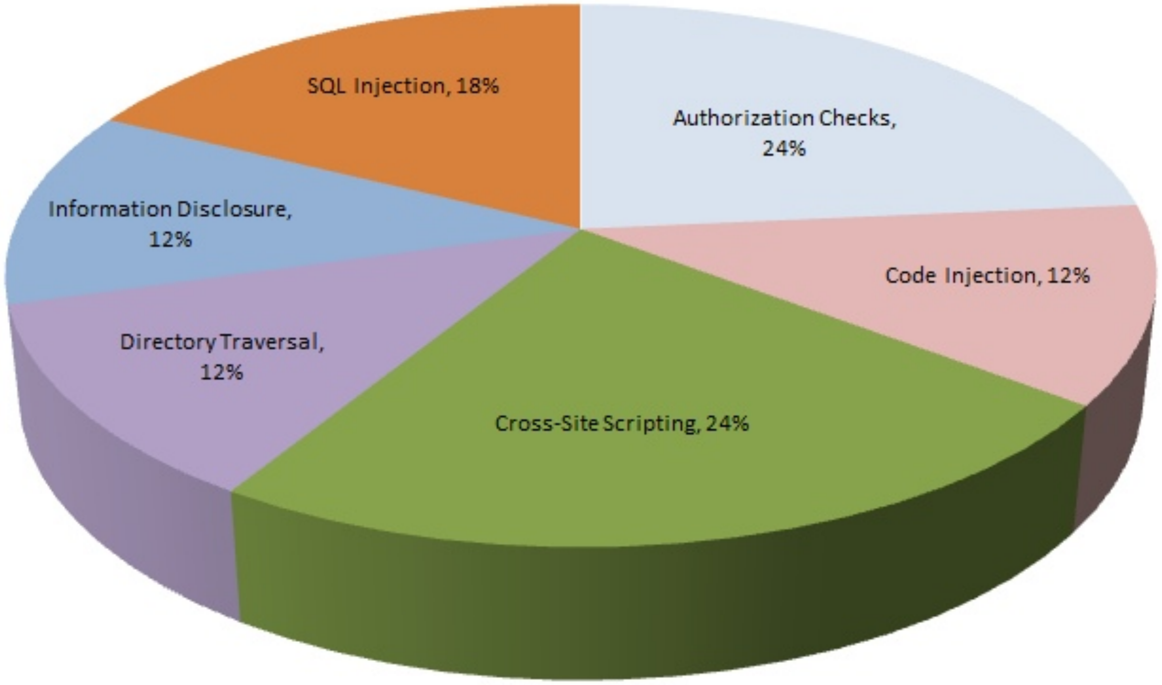
SAP Security Notes

October 2013

As a rule, Security Notes for missing or broken authorization checks are the most common form of patches released by SAP. However, during the month of October, SAP issued more patches for injection vulnerabilities affecting various components of its software than Notes addressing risks in application-level access. This includes the External List Management (EAL) component of SAP CRM used to procure, validate and administer contact lists containing information related to customers and partners (Note 1902162). It also includes BC-DB-MSS, used to monitor and administer the Microsoft SQL Server database (Note 1902854), MFG-ME, a solution that integrates business systems to control manufacturing processes (Note 1700224), and LO-MAP, a component of SAP Retail that supports merchandise and assortment planning (Note 1794273).

In common with other systems that rely upon relational database management systems to store business information, SAP systems are vulnerable to attacks that target SQL statements used to store and retrieve such information. SQL injection attacks involve the manipulation of character strings in SQL commands that are used to change the semantics of SQL statements such as SELECT, MODIFY, UPDATE, INSERT, and DELETE. Such tampering with SQL commands often occurs through malicious user input in forms and URLs, resulting in the disclosure of sensitive information, denial of service, privilege escalation and/or unauthorized changes to database records. It can also lead to code injection in scenarios where attackers are able to append or insert new database commands into vulnerable code including the SQL command EXECUTE.

Both ABAP and Java programs can be susceptible to injection attacks. Effective counter-measures include validation of user input which can also be used to neutralize cross-site scripting, directory traversal and other attacks. Validation can be performed



SAP Security Notes
by Vulnerability Type

against whitelists containing expected values for user-supplied entries. Since clients are untrusted, validation should be server-side. User supplied values in SELECT statements should be filtered to avoid injection vulnerabilities that threaten the confidentiality, integrity and availability of information in the entire database.

Customers are advised to implement the correction instructions supplied by SAP for the effected components. In accordance with the general guidance on patching issued by SAP in July this year, Security Notes flagged with priority 1 and 2 should be corrected within the standard patch cycle. Corrections for vulnerabilities reported by Notes identified as priority 3 and 4 can be applied through support packages.

Appendix: SAP Security Notes, October 2013

PRIORITY	NOTE	AREA	DESCRIPTION
2	1898055	SV-SMG-SYS	Missing authorization check in SV-SMG-SYS
2	1876343	BC-SRV-KPR-DMS	Missing authorization check in BC-SRV-KPR-DMS
2	1868140	BC-CST	Missing authorization check in SAP BASIS
2	1853616	XX-IDES	Missing authorization check in XX-IDES
2	1902162	CRM-MKT-EAL	Code injection vulnerability in CRM-MKT-EAL
2	1885371	BW-BEX-OT	Code injection vulnerability in BW-BEX-OT
2	1911067	BC-ESI-UDDI	Unauthorized modification of displayed content in ESREGBASIC
2	1828991	BC-XI-IS-WKB	Unauthorized modification of displayed content in RWB
2	1828988	BC-XI-IS-WKB	Unauthorized modification of stored content in RWB
2	1700735	MFG-ME	Unauthorized modification of displayed content in SAP ME
2	1863491	SV-SMG-MON-BPM	Directory traversal in SV-SMG-MON-BPM
2	1700733	MFG-ME	Directory traversal in SAP ME
2	1854826	BC-CTS-SDIC	Potential information disclosure for NetWeaver web sessions
2	1902854	BC-DB-MSS	Potential modif./disclosure of persisted data in BC-DB-MSS
2	1700224	MFG-ME	Potential modif./disclosure of persisted data in SAP ME
3	1914778	BC-DB-HDB-XS	Potential information disclosure relating to HANA host names
3	1794273	LO-MAP	Persisted data in MAP may be changed/disclosed

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

SAP Partner

Layer Seven Security offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Layer Seven Security makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.