ADVISORY

Layer Seven Security

SAP Security Notes

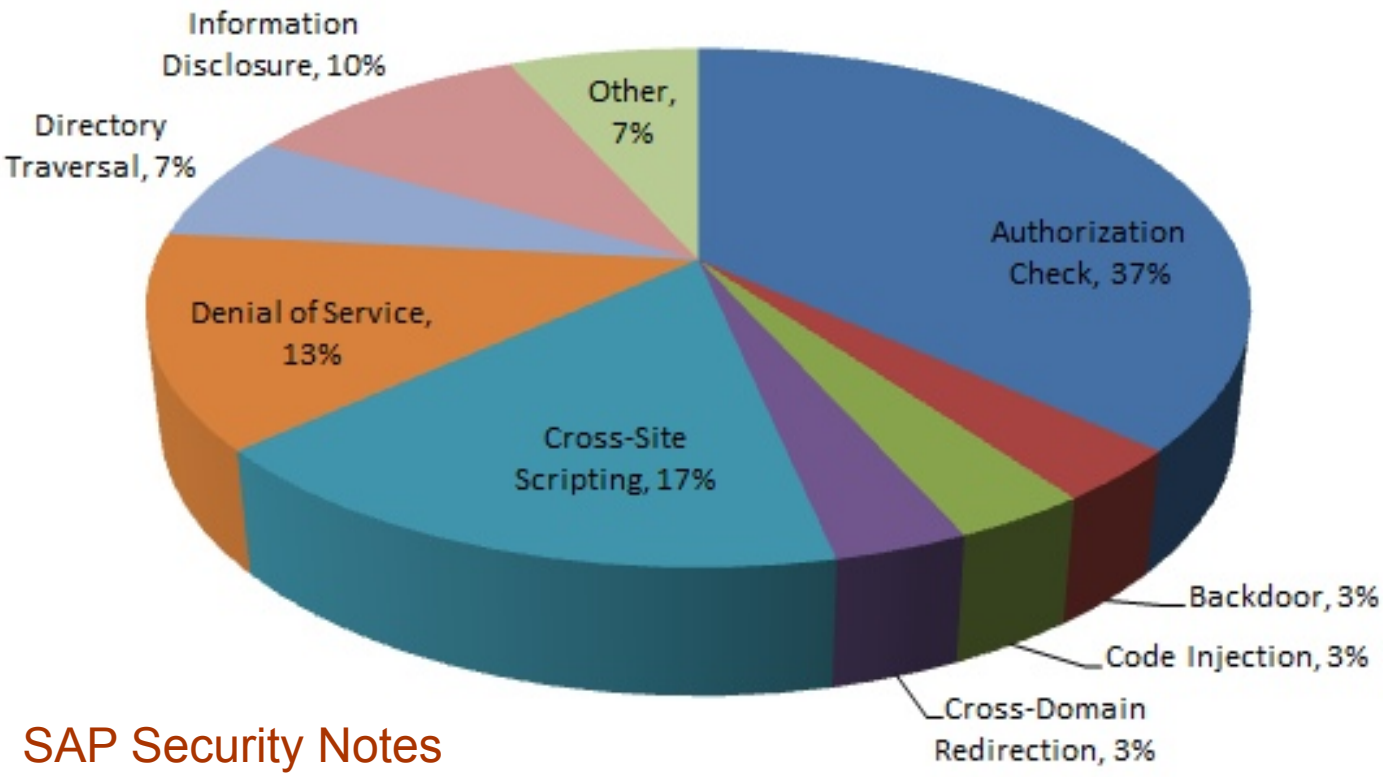
May 2013

SAP Security Notes

May 2013

In May, SAP released a critical patch for the SAProuter, used to control network connections to SAP systems. SAProuter is an optional but highly recommended program provided by SAP to complement port filters such as firewalls. It provides an additional layer of network-level protection by acting as an application-level gateway or proxy server to local area networks comprised of clustered SAP systems. The program improves overall security by enforcing password protection, encryption and authentication. The latter two are applied through the SNC layer. SAProuter uses a route permission table to regulate connections between source and destination hosts based on hostname, IP address or subnet. It will be permit, secure or deny connection attempts using the first match principle. Note 1820666 deals with a dangerous buffer overflow vulnerability in the SAProuter that could enable attackers to shut down, alter or corrupt the program through remote code execution. This may be used to change permission tables and allow unauthorised connections to SAP systems. As a result, customers are urged to install the latest version of SAProuter referenced in the Note.

Note 1416085 introduced an important change to the maintenance of the authorization object S_RFCACL. This object is used to control RFC connections based on trust relationships. S_RFCACL is a prerequisite for trusted RFC connections that do not require password authentication. The object includes several fields including RFC_SYSID, RFC_CLIENT and RFC_USER. These specific fields refer to the system ID, client and user ID of the calling system, respectively. The use of a wildcard (*) in these fields will enable logon from any system, client or user. Given the security risks arising from such a scenario, Note 1416085 removed all automatic methods of assigning full authorizations in these fields. After the implementation of the Note, Administrators can only assign wildcards manually through Profile Generator (PFGC) after accepting a system-generated warning message.



SAP Security Notes by Vulnerability Type

Information disclosure vulnerabilities generally do not rank high on vulnerability scales. Note 1823566 is no exception with a base CVSS score of only 4.0. However, this specific Note should be given close attention since it relates to an information disclosure vulnerability in the Solution Manager. Given that the Solution Manager stores information related to all systems in SAP landscapes, an information disclosure vulnerability in this component should be considered more closely than similar vulnerabilities in other components. Note 1823566 patches a flaw that could be exploited to discover database user passwords through the Solution Manager. The flaw arises from the storage of user names and passwords in the identical table. The Note introduces a new storage model that separates the columns into separate tables.

Customers using SAP's Extended Computer Aided Test Tool (eCATT) for functional testing should implement Note 1729638. This removes a hard-coded user in the program's source code which could be exploited to obtain unauthorised access to eCATT or escalate privileges and potentially alter test cases or results.

Appendix: SAP Security Notes, May 2013

PRIORITY	NOTE	AREA	DESCRIPTION
2	1812645	IS-A-JIT	Missing authorization check in JIT
2	1820033	BC-SYB-ASE	Potential denial of service in ASE Web Services and SCC
2	1820666	BC-CST-NI	Potential remote code execution in SAProuter
2	1823566	BC-DB-DBI	Potential information disclosure relating to SolutionManager
2	1826667	FIN-FSCM-TRM-TM	Missing authorization check in Treasury
2	1828465	FIN-FSCM-TRM-TM	Missing authorization check in Treasury
2	1828883	BC-SRV-BRF	Missing authorization check in BC-SRV-BRF
2	1833196	FS-BP	Missing authorization check in Business Partner
2	1837030	BC-CCM-PRN	Missing authorization check in SAP Printing
2	1839758	CA-GTF-SCM	Missing authorization check in CA-GTF-SCM
2	1840970	BI-BIP-AUT	Unauthorized modification of displayed content in InfoView
2	1718145	FS-CM	Missing authorization check in FS-CM
2	1729638	BC-TWB-TST-ECA	Hard-coded credentials in eCATT
2	1741239	BC-WD-ABA-REN	Directory traversal in Web Dynpro ABAP
2	1751310	BC-DB-SDB-CCM	Potential information disclosure relating to parameters
2	1779578	BC-ESI-WS-JAV-RT	Directory traversal in ENGINEAPI
2	1787455	BC-DB-LCA	Missing authorization check in LiveCache Applications
2	1803097	FIN-FSCM-TRM-TM	Missing Authorization Check in TRM Transaction Management
2	1810809	BC-CCM-SLD	Potential uploading of malicious files in SLD
3	1864086	FIN-BA	Update 1 to Security Note 1665930
3	1826123	BI-RA-WBI	Unauthorized modification of stored content in web tier
3	1829584	BC-DB-ORA-CCM	Potential information disclosure related to BRBACKUP
3	1833139	BI-BIP-BIW	Potential false redirection of Web site content in EPM
3	1416085	BC-SEC-AUT-PFC	PFCG: Authorization maintenance for object S_RFCACL
3	1562782	GRC-SPC	Missing authorization check in GRC-SPC
3	1723018	BC-MID-ICF	Unauthorized modification of displayed content in ICF
3	1772370	EP-KM-CM-UI	Untrusted XML input parsing possible in KM UI
3	1790213	EP-PIN-TOL	Unauthorized modification of stored content in Themes area
3	1791238	BC-ABA-SC	Potential denial of service in SAP Kernel (Diag parser)
3	1791490	BC-ABA-SC	Potential denial of service in SAP Kernel (Diag parser)

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