ADVISORY

Layer Seven Security

SAP Security Notes

June 2013

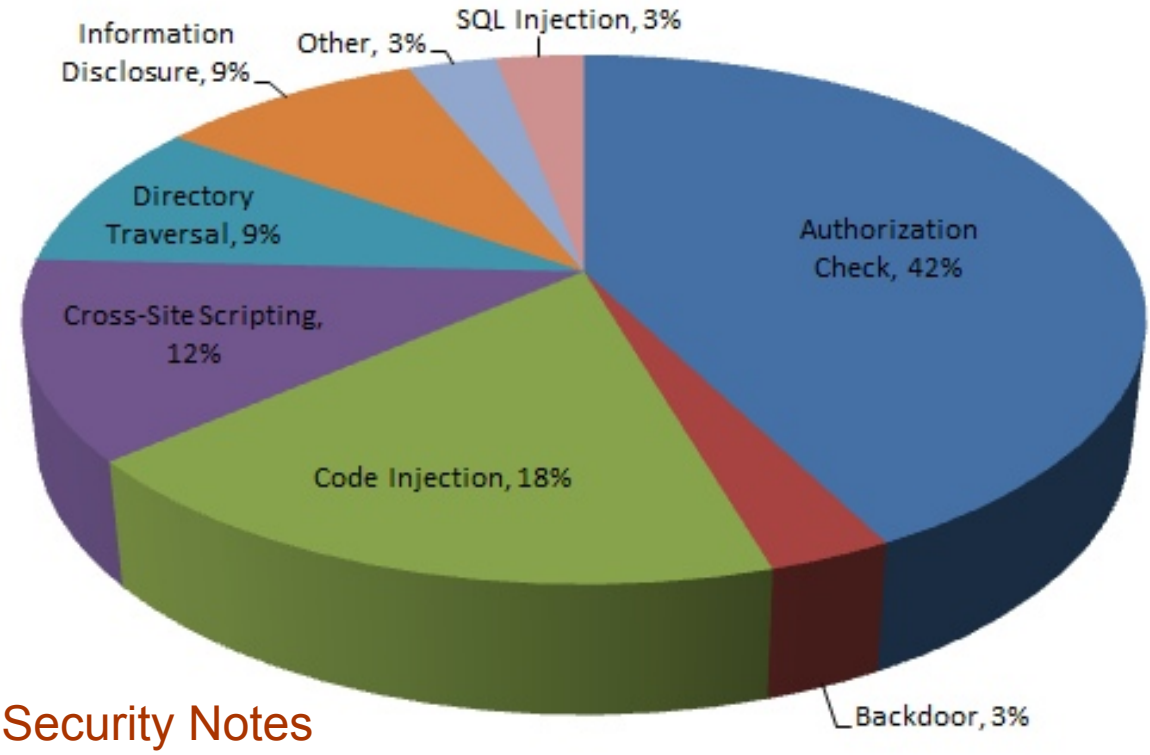
SAP Security Notes

June 2013

SAP released several patches for multiple vulnerabilities effecting Sybase EAServer in June. EAServer is used to create, deploy and configure Java servlets, JavaServer Pages and Web applications. The latter is enabled through the support of common standards for Web Services including the Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and Uniform Description, Discovery and Integration (UDDI). EAServer enables organizations to expose stored procedures in systems such as Sybase ASE, SQL Anywhere, IQ and other databases as Web services. It is also used to load balance between clustered application servers, define database types and data sources and perform other administrative and monitoring tasks.

The EAServer vulnerabilities were discovered by security researchers Gerhard Wagner and Bernhard Mueller of SEC Consult Vulnerability Lab. SAP was notified in November last year. The vulnerabilities include OS command injection (Note 1851914), directory traversal (Note 1852064) and information disclosure (Note 1858107). Note 1851914 is rated the most critical and carries a CVSS score of 10.0. An external entity (XXE) vulnerability in EAServer caused by a lack of input validation can enable attackers to list directories and files on target systems. This can lead to the unauthorized retrieval of administrative credentials from configuration files which can then be used to execute OS commands through the WSH service. Customers are advised to update their EAServer installation as soon as possible through the application of the appropriate EBF for their platform.

Note 1853161 relates to a privilege escalation vulnerability in the ABAP Editor, a source code editing tool and component of ABAP Workbench. ABAP Editor is used to develop and modify programs, function modules and other objects.



SAP Security Notes by Vulnerability Type

This should only be permitted for users granted a unique developer license key, stored in the table DEVACCESS. Note 1853161 patches a vulnerability in Workbench that led to the failure to request developer access keys for the some functions performed through ABAP Editor.

Other important patches include Note 1805024, which deals with a missing authorization check for the maintenance of configuration parameters in SAP profiles, and Notes 1831985 and 186098 that deal with command injection and cross-site scripting vulnerabilities in NetWeaver Identity Management (IdM). The command injection vulnerability could lead users to escalate privileges and assign permissions without authorizations.

The cross-site scripting vulnerability can lead to session hijacking through weaknesses in the REST interface. As a result, SAP recommends disabling the interface or restricting access to the interface for specific versions of AS Java.

Appendix: SAP Security Notes, June 2013

PRIORITY	NOTE	AREA	DESCRIPTION
1	1851914	BC-SYB-EAS	Potential remote code execution in EAServer
2	1820777	BC-JAS-ADM-ADM	Update 1 to SAP security note 1755108
2	1838814	PLM-CFO	Unauthorized modification of stored content in cFolders
2	1842218	PS	Missing authorization check in PS
2	1842406	BC-CST-IC	Missing authorization check in in package SICM
2	1843082	BC-SEC	Missing authorization check in RSDUMPSOURCE
2	1844202	BC-SEC-USR-IS	SUIM| RSUSR002 User '.....' is not found
2	1847645	BC-BMT-WFM	Missing authorization check in BC-BMT-WFM
2	1848319	BC-ABA-TV	Missing authorization check in BC-ABA-TV
2	1848996	BC-ILM-LCM	Missing authorization check in BC-ILM-LCM
2	1849559	BW-WHM-DST	Code injection vulnerability in BW-WHM-DST
2	1849744	EP-BC-UWL	Missing authorization check in SAP_BASIS
2	1852064	BC-SYB-EAS	Directory traversal in EAServer
2	1853161	BC-DWB-TOO-FUB	Privilege Escalation in ABAP Source Code Editor
2	1853852	IS-B-BCA	Missing authorization check in IS-B-BCA
2	1858107	BC-SYB-EAS	Potential disclosure of persisted data in EAServer
2	1781594	BC-SRV-ALV	Code injection vulnerability in component BC-SRV-ALV
2	1805024	BC-CCM-CNF-PFL	Missing authorization check in SAP profile functions
2	1816331	BC-SRV-ALV	Code injection vulnerability in BC-SRV-ALV
2	1826162	BC-SRV-COM-FTP	Update 1 to security note 1674132
2	1831463	BC-UPG-TLS-TLA	Potential modification of persisted data in upgrade tools
2	1831985	BC-IAM-IDM	Command injection vulnerability in SAP Netweaver IdM
2	1834935	LO-GT-TEW	Missing authorization check in LO-GT-TEW
2	1835666	SCM-APO-INT-MD-PDS	Missing authorization check in PDS_MAINT

Appendix: SAP Security Notes, June 2013 cont.

PRIORITY	NOTE	AREA	DESCRIPTION
2	1836717	BW-BEX-ET	Hard-coded profiles in BW-BEX-ET
3	1846952	EPM-BPC-NW	Missing authorization check in BPC Web Services
3	1630309	CRM-IC-FRW-UI	Unauthorized modification in BSP application in CRM-IC-FRW
3	1753737	BI-BIP-BIW	Unauthorized modification of displayed content in BOE
3	1774270	LO-MD-MM	Update 1 to security note 1500050
3	1774432	SV-SMG-SDD	Missing authorization check in ST-PI
3	1806098	BC-IAM-IDM	Unauthorized Use of Application Functions in REST Interface
3	1816989	EP-PIN-CS	Potential information disclosure relating to EPCM data bag
3	1822847	BC-XI-IBC	Potential information disclosure in PI

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