Layer Seven Security

ADVISORY

SAP Security Notes

September 2013

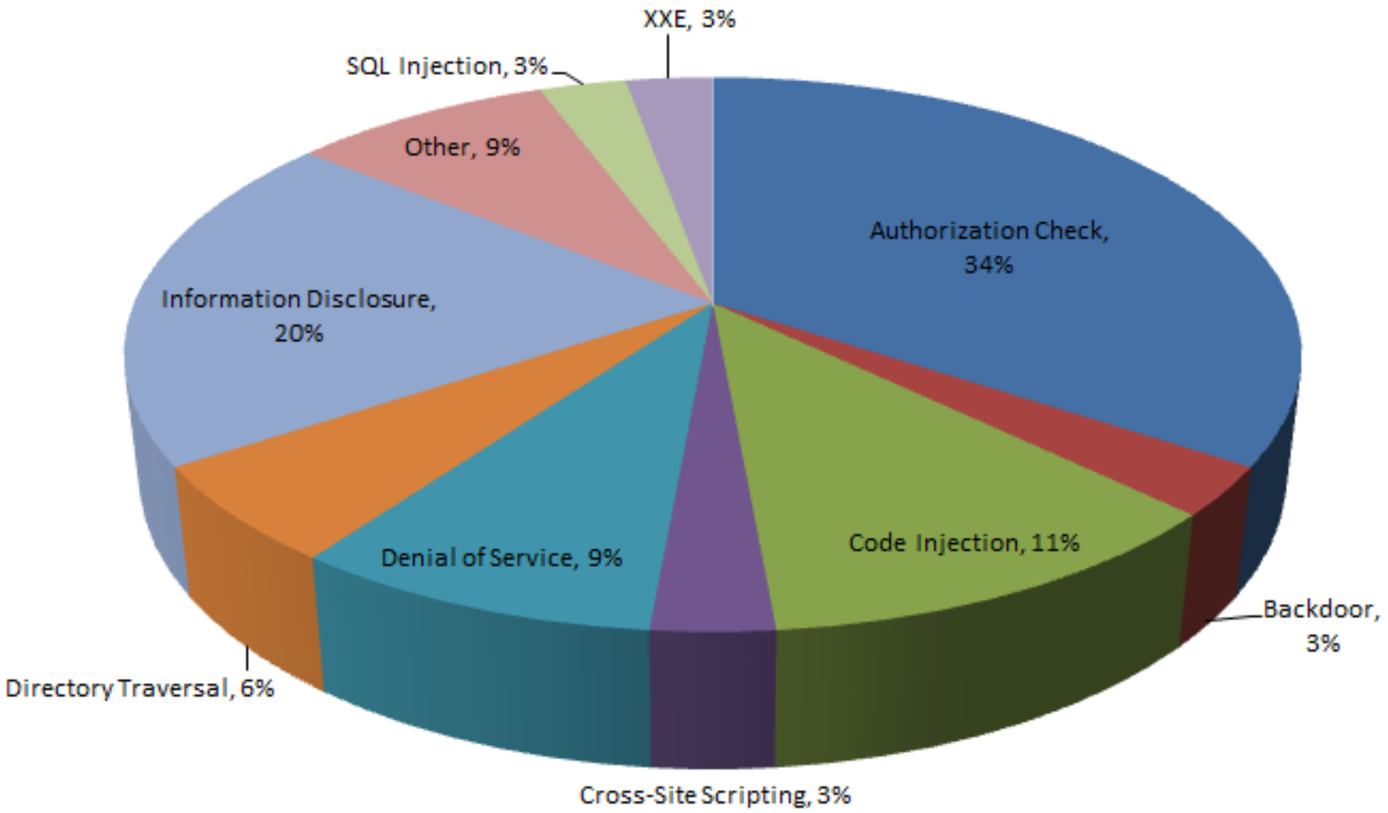
SAP released a series of patches in September for the Adaptive Server Enterprise (ASE) relational database management system developed by Sybase, a company acquired by SAP in 2010. ASE is Sybase's flagship database server, available in both Unix and Windows variants. Most of the patches released for the ASE were a response to vulnerabilities identified by external researchers including TeamShatter at Application Security Inc (AppSecInc). TeamSHATTER is no stranger to Sybase. The research group issued an urgent notice last year for twelve vulnerabilities it had identified in Sybase components. According to TeamSHATTER, only two of the issues reported to Sybase in 2012 were effectively resolved by subsequent patches. In it's words, "With very minor modifications to the original proof of concept code TeamSHATTER sent to Sybase in our initial vulnerability report, the exploits still work. It appears that Sybase blocked the specific exploit code we submitted without fixing the underlying vulnerability, and then performed insufficient testing and code review to notice the problem before shipping the patches and publicly disclosing the vulnerability information." (http://www.teamshatter.com/topics/general/team-shatter-exclusive/sybase-disclosed-but-unpatched-vulnerabilities/).

The attack signatures for the exploits discovered by TeamSHATTER were incorporated into AppSecInc's knowledgebase of database vulnerabilities. Layer Seven Security leverage security tools developed and supported by AppSecInc to identify and remove misconfigurations and other exploits in database platforms. Therefore, our customers were able to protect their database resources through alternative measures prior to the release of the Security Notes for Sybase, regardless of the effectiveness of such patches.

SAP Security Notes

September 2013

TeamSHATTER have yet to comment on the most recent patches released by Sybase in response to its research. The most



SAP Security Notes by Vulnerability Type

significant are intended to counter buffer overflow vulnerabilities that enable attackers to take complete control of the ASE including the modification or deletion of all data (1893560 and 1893558). Other vulnerabilities in the ASE addressed by Security Notes released in September include SQL injection (1893440), directory traversal (1893556), denial of service (1887342, 1893561), information disclosure (1887341, 1893562, 1809246), and missing authorization checks (1849356).

Note 1879601 provides instructions for securing network access to the enqueue server, used to manage lock requests and collisions in SAP work processes. SAP recommends blocking access to the enqueue server from the client network. Access should only be enabled from components in the server network. This can achieved through network firewalls or ACLs configured in the parameter *enque/acl_file*.

Finally, Note 1871683 provides recommendations for patching a denial of service vulnerability in the SAP Security Audit Log. The successful exploitation of this vulnerability could lead to the failure to log and notify administrators of significant security events such as changes to user master records and specific dialog or RFC logons. In response, SAP recommends either implementing the relevant support package for the applicable release or a manual correction within each system. The latter involves modifying the severity level of the AV5 system log message through transaction SE92.

Appendix: SAP Security Notes, September 2013

PRIORITY	NOTE	AREA	DESCRIPTION
1	1893560	BC-SYB-ASE	Potential remote code execution in SAP Sybase ASE
2	1881914	BC-DB-ORA-CCM	Code injection vulnerability in BC-DB-ORA-CCM
2	1884512	IS-A-ESD	Missing authorization check in IS-A-ESD
2	1885611	FS-SR	Code Injection vulnerability in FS-SR
2	1887341	BC-SYB-ASE	Potential information disclosure relating to SAP Sybase ASE
2	1888563	IS-B-BCA	Missing authorization check in IS-B-BCA
2	1889895	BC-CUS-TOL-BCD	Missing authorization check in BC-CUS-TOL-BCD
2	1890819	SV-SMG-DIA	Untrusted XML input parsing possible in Hotspot Analysis
2	1893440	BC-SYB-ASE	Elevation of privileges in SAP Sybase ASE
2	1893556	BC-SYB-ASE	Directory traversal in SAP Sybase ASE
2	1893558	BC-SYB-ASE	Potential remote code execution in SAP Sybase ASE
2	1896785	SV-SMG-SDD	Missing authorization check in ST-PI
2	1879601	BC-CST-EQ	Secure setup of the standalone enqueue server
2	1672911	BC-SRV-NBC	Hard-coded credentials in BC-SRV-NBC
2	1766044	SD-BIL-IV-SM	Missing authorization checks for enhanced contract data
2	1777053	BC-SEC-USR-ADM	Missing authorization check in BC-SEC-USR-ADM
2	1782955	BC-JAS-SEC	Missing authorization check in the telnet command password
2	1783795	BC-CTS-CCO	Potential disclosure of persisted data in [BC-CTS-CCO]
2	1828801	SV-SMG-DIA-SRV-AGT	Unauthorized modif. of displayed content in SV-SMG-DIA-SRV
2	1831932	BC-XI-CON-B2B-AS2	Missing authentication in AS2 Adapter
2	1842826	BC-SRV-KPR-DMS	Missing authorization check in BC-SRV-KPR-DMS
2	1847590	BC-SRV-KPR-RET	Missing authorization check in BC-SRV-KPR-RET
2	1860258	IS-A-ESD	Missing authorization check in IS-A-ESD
2	1863278	BC-SRV-ALV	Missing authorization check in BC-SRV-ALV (miniALV)
2	1871683	BC-SEC-SAL	Potential denial of service in Security Audit Log

Appendix: SAP Security Notes, Sept. 2013 cont.

PRIORITY	NOTE	AREA	DESCRIPTION
3	1887342	BC-SYB-ASE	Potential denial of service in SAP Sybase ASE
3	1888167	BC-DWB-TOO-RTA	SMB Relay in Runtime Analysis
3	1888502	BC-CCM-PRN-TMS	SMB Relay in Temse
3	1893561	BC-SYB-ASE	Potential denial of service in SAP Sybase ASE
3	1893562	BC-SYB-ASE	Potential information disclosure relating to SAP Sybase ASE
3	1779676	WEC-APP-UM	Potential information disclosure in contact scenario
3	1786809	PY-NO	Directory traversal in PY-NO
3	1809246	BC-SYB-ASE	Potential information disclosure relating to SAP Sybase ASE
3	1849356	BC-SYB-ASE	Missing authorization check in SAP Sybase ASE
3	1864915	CRM-ISA-BBS	Potential information disclosure relating to CRM-ISA-BBS

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.

This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

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.