Layer Seven Security

ADVISORY

SAP Security Notes

December 2012

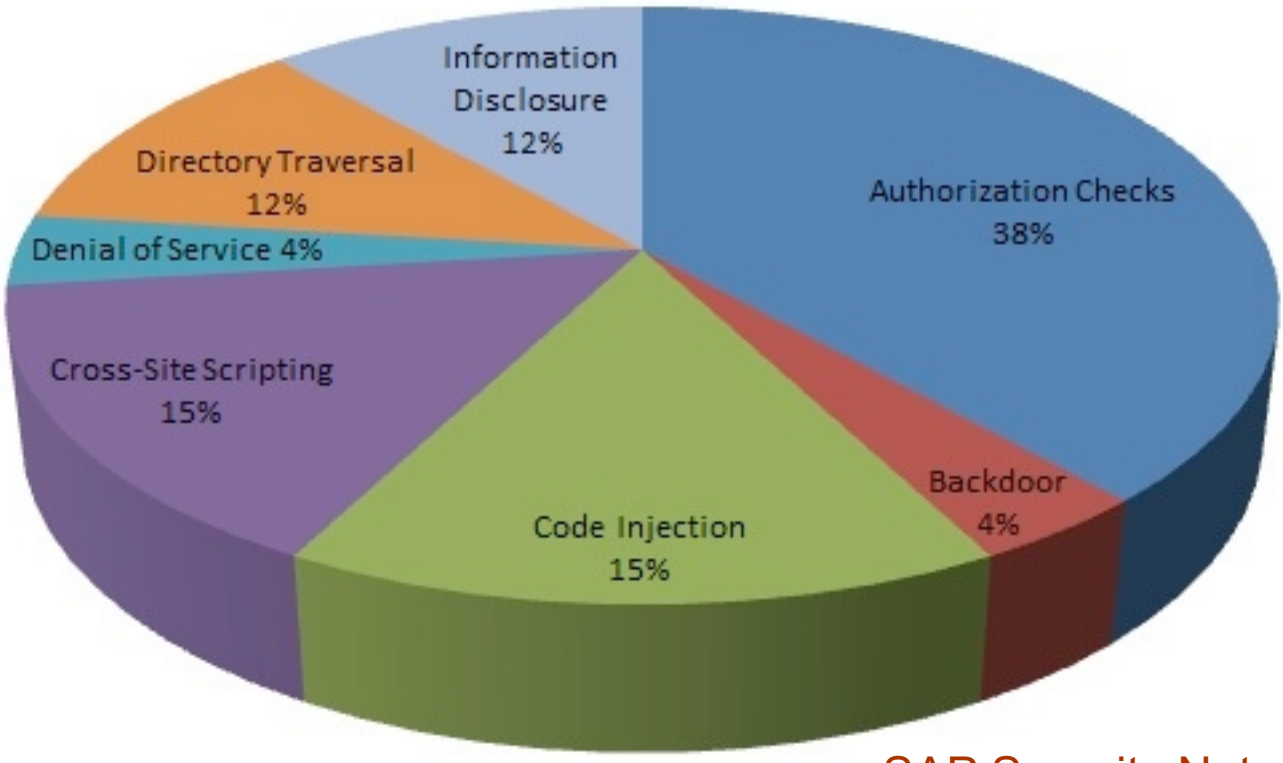
SAP Security Notes

December 2012

In November, SAP released an unusually high number of Security Notes to patch various forms of injection vulnerabilities in it's software. The trend continued in December with the release of several patches for code injection flaws in the Computer Center Management System (BC-CCM), Project System (PS-IS), Transport Organizer (BC-CTS-ORG) and work processes in Application Servers responsible for executing ABAP programs (BC-CST). Given this alarming trend, this advisory is focused on discussing the challenges of developing secure ABAP programs for SAP systems, free of common vulnerabilities including not only injection flaws, but cross-site scripting errors, buffer overflows, directory traversals and backdoors and rootkits.

There are three attack surfaces in SAP systems. The first is through improperly defined and controlled application-level access. This attack surface is the most commonly known and understood by SAP customers. Today, most SAP clients deploy any one of a variety of access management tools to control access to sensitive functions and maintain a strict segregation of duties in their ERP systems. This manages the risk of unauthorized access through inadequate authorization structures that grant excessive or conflicting privileges to users and administrators.

The second attack surface lies at the platform level. This generally refers to components of the NetWeaver Application Server, also referred to as the Basis area of SAP systems. The NetWeaver AS is the technical foundation of the entire SAP software stack. It provides the runtime environment for SAP applications and includes work processes for ABAP and Java programs, gateways and modules for managing RFC, Web-based and other forms of communication protocols, tools to manage user roles, profiles and authorizations, and utilities that control certain database and operating system functions.



SAP Security Notes by Vulnerability Type

The secure configuration and management of the NetWeaver AS is a vital component of a comprehensive SAP security strategy. However, the results of our security assessments repeatedly reveal common vulnerabilities in basis settings in most SAP environments. This provides a lush attack surface to internal and external attackers looking for an avenue to manipulate or appropriate business data or deliberately disrupt the availability of SAP systems.

The third and final attack surface in SAP provides an even greater array of opportunities for attackers. This surface exists at the program level. ERP systems such as SAP are designed to perform thousands of distinct functions ranging from, for example, adding a vendor to a list of approved suppliers, performing a transport to implement a change in a specific system, or encrypting/ decrypting traffic between servers or clients. These functions are performed by programs stored in the database table known as REPOSRC that are called when requested by work processes in the NetWeaver AS.

SAP programs are developed using two distinct programming languages: Advanced Business Application Programming (ABAP) and Java. Both are vulnerable to coding errors that could expose SAP programs to exploits such as code, OS and SQL injection, cross-site scripting, cross-site request forgery, buffer overflow, directory traversal and denial of service. SAP programs are also susceptible to missing or broken authority-checks that could lead to unauthorized execution of programs. Finally, SAP programs can contain backdoors through hardcoded credentials that bypass regular authentication and authorization controls, as well as malware known as rootkits that provide attackers with remote, privileged access to system functions and resources.

Custom programs should be subject to the same level of review performed by SAP for standard programs

SAP performs a rigorous code review for all standard or delivered programs prior to release. However, some of the vulnerabilities present in the code base are not detected and patched until after release. Security Notes are therefore an important mechanism used by SAP to patch vulnerabilities arising from programming errors.

Custom programs are rarely subject to the same level of scrutiny applied by SAP to standard programs. Programs developed by in-house or off-shore developers to meet the needs of customers not met by standard SAP functionality are often laden with vulnerabilities that, when exploited, undermine the integrity of entire SAP landscapes. Such landscapes are only as strong as their weakest point. A robust application layer fortified with GRC tools has led attackers to shift their focus to the platform and code level. Given the relative openness of most SAP systems at the technical level, the strategy is proving to be profitable.

SAP has responded by issuing a series of recommendations to customers to strengthen configuration settings in components of the NetWeaver AS. These can be found in the whitepaper *Secure Configuration of the SAP NetWeaver Application Server Using ABAP.*

However, understandably SAP is less vocal on development procedures for custom programs since this is generally the responsibility of each SAP customer. The challenge should not be underestimated. Although manual code reviews to detect common vulnerabilities are theoretically possible, the skill-set to effectively review custom code is not only rare but expensive. Furthermore, it often leads to an increase in development time. Customers should consider investing in code scanning tools that are tuned to detect suspicious statements in ABAP code and integrate directly into the SAP Transport Management System (TMS). Such tools should also be capable of auto-correcting ABAP statements to minimize resource requirements and the impact on existing development times. Presently, the only tool capable of detecting and auto-correcting vulnerabilities in custom ABAP programs, with direct integration with SAP TMS, is Virtual Forge CodeProfiler. To arrange a security scan of custom programs in your SAP environment using CodeProfiler, please contact a representative at Layer Seven Security.

Appendix: SAP Security Notes, December 2012

PRIORITY	NOTE	AREA	DESCRIPTION
2	1769099	BC-DOC-TER	Update 1 to security note 1541716
2	1771020	BC-CCM-PRN	Code injection issue in BC-CMM-PRN
2	1771149	FS-CM	Directory traversal in FS-CM: Claims Management
2	1771204	CA-GTF-SCM	Missing authorization check in CA-GTF-SCM
2	1772498	BC-BMT-OM	Missing authorization check in BC-BMT-OM
2	1773758	BC-CST	Code injection vulnerability in TH_ENQUEUE_PERF
2	1774903	BC-CST	Hard-coded logon information in taskhandler
2	1775171	XX-PROJ-FI-CA	Directory traversal in FI-CA
2	1775317	IS-PS-CA	Directory traversal in IS-PS-CA
2	1776695	PS-IS	Code injection vulnerability in PS-IS
2	1424979	SCM-APO-MSP	Security Check: Call transaction authorization checks
2	1426028	SCM-BAS-MD-RE	Security Check: Call transaction authorization checks
2	1429094	SCM-APO-INT-MD-PDS	Missing authorization check in SCM PDS Integration
2	1429098	SCM-APO-PPS	SCM Security Check: Missing Authority Check
2	1429154	SCM-APO-PPS-PCM	SCM Security Check: Missing Authority Check
2	1430757	SCM-BAS-UIF	Super user feature in SNC
2	1486380	BC-XI	Potential information disclosure relating to users and pwds
2	1659874	BC-XI-CON-AFW	PI SEC: Missing authorization check in PI Adapter Framework
2	1714607	BC-CTS-ORG	Code injection vulnerability in SAP_BASIS
2	1724623	AIE-AII-UI	Missing authorization check in AutoID Mobile applications
3	1746074	EP-KM-CRS	Unauthorized modification of stored content in EP-KM-CRS
3	1751800	CRM-ISA-BCS	Potential information disclosure relating to CRM-ISA-BCS
3	1756727	CRM-LOY-MSH	Invalid authorization check for Loyalty component
3	1689059	BW-BEX-ET-WJR-RT	Unauthorized modification of displayed content in BEx Web
3	1707298	BC-SRV-KPR-DMF	Update#2 to Security note 1579673
3	1743377	EP-PIN-APF	Unauthorized modification of displayed content in EP-PSERV

Layer Seven Security

Layer Seven Security specialize in SAP security. We serve customers worldwide to protect information assets against internal and external threats and comply with industry and statutory reporting requirements. The company fuses technical expertise with business acumen to deliver unparalleled implementation, consulting and audit services targeted at managing risks in contemporary SAP systems.

Layer Seven Security leverage leading SAP-certified software to deliver end-to-end assessments that detect and remediate vulnerabilities at all levels in SAP landscapes.

The company is privately owned and headquartered in Toronto, Canada.

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