ADVISORY

Layer Seven Security

SAP Security Notes

April 2013

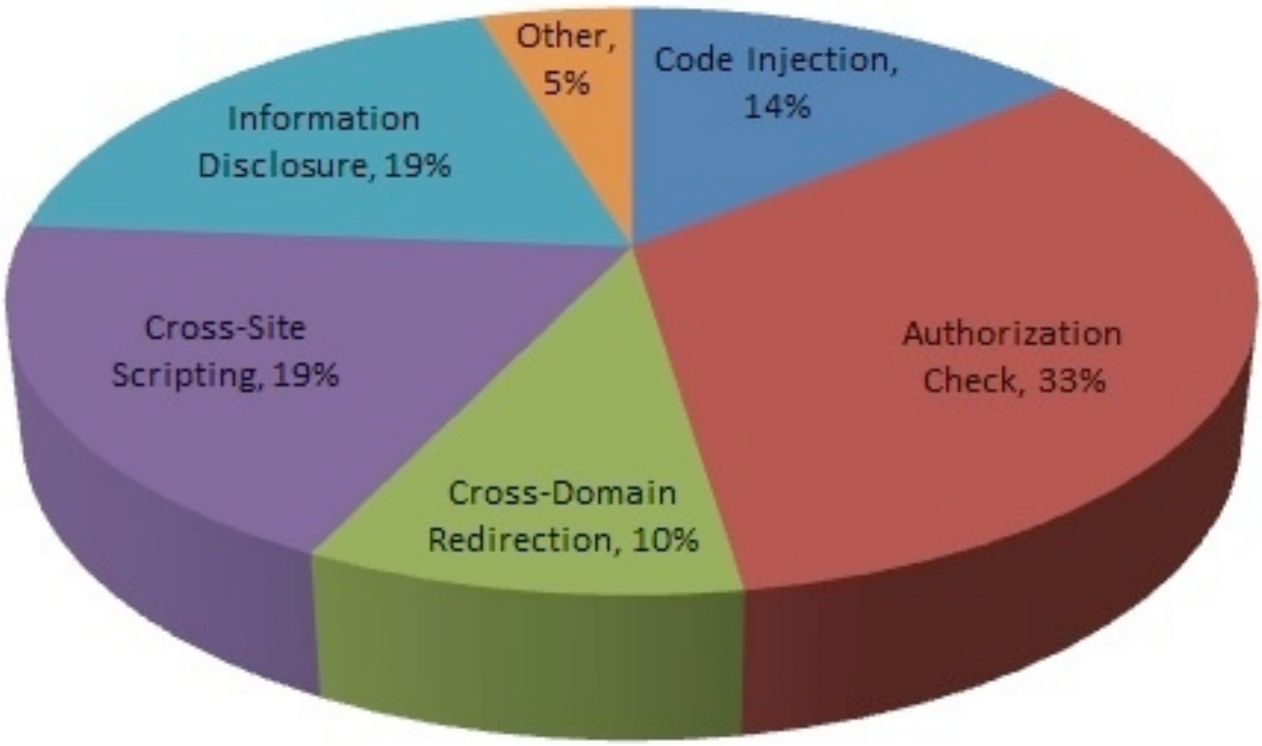
SAP Security Notes

April 2013

April's list of Security Notes included the usual patches for missing authorization checks, cross-site scripting flaws, information disclosure vulnerabilities and updates for existing Security Notes. The affected components primarily covered areas within Business Connector (BC) used to integrate SAP systems with non-SAP systems through open standards and technology, and Business Intelligence (BI), a platform supporting information analysis and reporting. However, one specific Security Note deserves particular attention: Note 1827217 deals with an OS command injection flaw in the ABAP runtime environment.

Injection flaws occur when external input is improperly neutralized or validated by programs, enabling attackers to introduce and execute malicious code in applications. Such code can include scripts or payloads designed to compromise entire systems and landscapes. Injected code is difficult to detect since it takes advantage of existing running processes. This also makes it invisible to anti-virus solutions. Malicious programs operating within enterprise applications take advantage of the trusted status conferred by AV systems to SAP processes. Commands made by attackers appear to originate from SAP applications trusted by AV systems. Injected code is also difficult to remove. Often, processes can't be disabled without shutting down entire systems.

There are several ways to perform OS commands in SAP systems. The standard method is via transactions SM49 and SM69 used to define and execute logical OS commands used for background processing, job scheduling and other functions. Customers should maintain a strict white list of permitted commands and restrict the ability of users to execute calls through the authorization object S_LOG_COM. This should include defining appropriate values for the fields *command, opsystem*, and *host*.



SAP Security Notes by Vulnerability Type

The authorization S_LOGCOM_ALL enables execution of all OS commands and is included in the standard profiles S_A.SYSTEM and S_A.ADMIN.

Lesser-known methods to execute OS commands in SAP include SYSTEM kernel-calls which allow the execution of calls not maintained in SM49 and SM69, and the ABAP command OPEN DATASET used to access files on SAP servers. The use of such methods is highly dangerous and should be avoided. SAP recommends the use of the ABAP function module COMMAND_EXECUTE rather than CALL_SYSTEM since the former avoids the use of RFC and supports more granular authorization checks.

OS command injection flaws are commonly ranked very high by vulnerability scoring scales such as CVSS. This is often due to the fact that breached applications are usually privileged programs with root or administrator level rights on host operating systems. SAP operates with system-wide privileges.

Similar to other injection flaws, OS command injection vulnerabilities can be prevented by minimizing user input through the use of library calls. Other measures can include input validation through whitelisting permitted ABAP commands, parameterization and output encoding. Application-level firewalls and gateways also provide some measure of protection.

Organisations that detect OS command vulnerabilities in custom programs through static code analysis should consider blocking access to vulnerable areas as a temporary stop-gap measure. SAP has gone one step further. The solution packaged with Note 1827217 leads to the complete deletion of the affected SAP program.

Appendix: SAP Security Notes, April 2013

PRIORITY	NOTE	AREA	DESCRIPTION
2	1847764	CA-EUR	Update 1 to security note 1795103
2	1845532	BC-CCM-MON	Update 1 to security note 1616366
2	1827217	BC-ABA-LA	Code injection vulnerability in ABAP Verification
2	1824792	FIN-FSCM-TRM-TM	Missing authorization check in Treasury
2	1821306	GRC-SAC-ARQ	End User logon authentication is bypassed in Access Request
2	1812581	CO-PC-PCP	Missing authorization check in CO-PC-PCP
2	1801585	BC-ABA-TO	Potential disclosure of persisted data in "ABAP Selections"
2	1784771	BI-BIP-ADM	Potential false redirection of Web site content in BOE
2	1757472	BC-GP	Potential information disclosure relating to Archive Monitor
2	1718022	FS-CM	Missing authorization check in FS-CM
2	1573173	BC-JAS-WEB	Potential disclosure of server related information
3	1821862	BC-CCM-PRN	SMB relay in BC-CCM-PRN
3	1821019	BC-CCM-CNF-PFL	Missing authorization check in package SPFL
3	1819822	BC-JAS-COR	Missing authorization check in configuration service
3	1816536	BC-CCM-HAG	Potential information disclosure relating to SAP Host Agent
3	1800926	BW-BEX-ET-WJR-RT	Unauthorized modification of displayed content in BW-BEX
3	1784833	BI-BIP-DEP	Potential false redirection of Web site content in BOE xir3
3	1784772	BI-BIP-LCM	Potential information disclosure relating to LCM
3	1762486	BI-BIP-DEP	Unauthorized modification of displayed content in BOE
3	1749111	BI-BIP-ADM	Unauthorized modification of displayed content in BOE
3	1744879	BC-FES-CTL	Unauthorized modification of stored content in Data Provider

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