Layer Seven Security

ADVISORY

SAP Security Notes

December 2013

SAP Security Notes

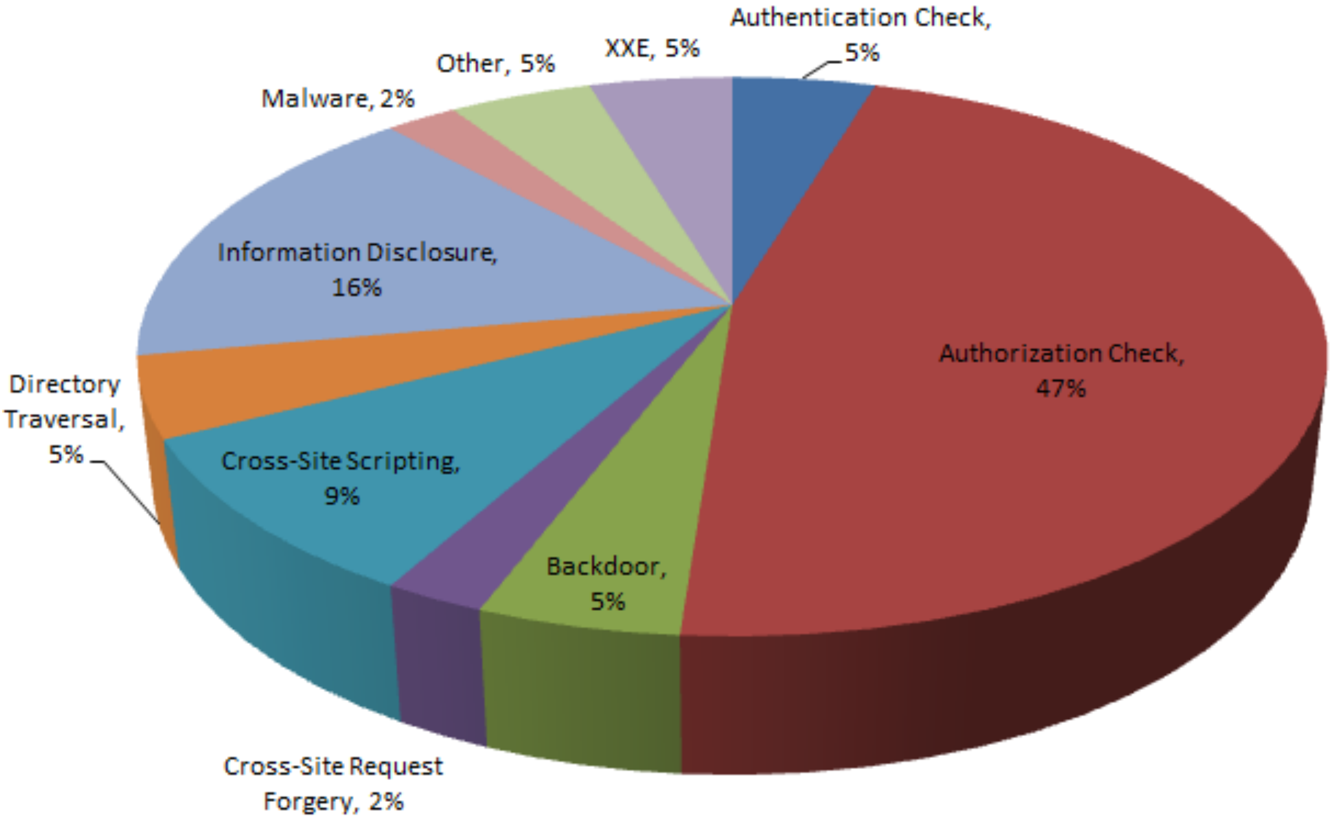
December 2013

SAP announced an important change to the release strategy for security patches in December. In order to respond more rapidly to externally reported vulnerabilities and critical security-related programming errors discovered through internal quality assurance efforts, Security Notes will no longer be released for most lower priority 3 and 4 vulnerabilities. Patches for such issues will be delivered primarily with support packages. Therefore, given that corrections for all security vulnerabilities are not provided exclusively through Security Notes, customers are advised to implement support packages as soon as they are available at the SAP Service Marketplace to maintain patch levels for SAP systems.

SAP also introduced a new rating scale for Security Notes in December. The previous four-tier priority model was replaced by a simplified three-tier approach. Security patches are now rated on a high-medium-low scale.

The catalyst for the changes may have been the variant of the carberp malware targeting SAP clients that was disclosed in November. The malware is capable of logging keystrokes and capturing screenshots which could lead to the theft of user credentials and other sensitive information related to SAP systems. The need to respond quickly to such a well-publicised event may have extended the already stretched security resources at SAP.

Note 1946009 includes numerous recommendations from SAP to counter the threat posed by the malware. This includes updating anti-malware and IPS signatures, restricting the administrative privileges of end users on local machines, installing OS patches and updates, enabling single sign-on, network and host-level firewalls, disabling AutoRun features, and avoiding the use of non-complex passwords across multiple systems and accounts.



SAP Security Notes by Vulnerability Type

Since the malware targets front-end SAP clients, customers should also consider hardening security policies for SAP GUI including disabling user scripting and input history, limiting multiple logons and enabling strong filtering rules in the SAP GUI security module.

Other important Notes include 1752717. This extends the Cross-Site Request Forgery (XSRF) Protection Framework to a component within the Manufacturing module that uses Servlets, JSPs and other Java specifications. The Framework was introduced in 2010 to combat XSRF attacks that attempt to send requests through compromised browsers to application servers using the credentials of trusted users. Applications that rely exclusively on automatically submitted credentials such as session cookies, certificates or username/password combinations are vulnerable to this form of attack since they are unable to distinguish between legitimate and malicious requests. The Framework applies tokens as an additional parameter to protect against XSRF attacks. The token is generated after logon and bound to the user session. Implementation instructions for the Framework are attached to Note 1450166.

Note 1931016 patches missing authorisation checks in the ABAP Runtime Analysis by introducing an S_TCODE check for transactions including SE30, SE30_OLD and SAT. The ABAP Runtime Analysis is a component of the ABAP Workbench used for source code performance analysis.

Missing authorization checks in other critical components are addressed by Notes 1773912 (message server), 1906927 (Accounting BAPIs) and 1776718 (password telnet command).

Appendix: SAP Security Notes, December 2013 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	1956501	PE-LSO-LPO	Update #1 to security note 1687668
HIGH	1882597	GRC-SAC-ARQ	UAM: End user login authentication not working properly
HIGH	1735125	SV-SMB-AIO-PFW-SB	Unauthorized modification of displayed content in BP-INSTASS
HIGH	1808706	SBO-IMCE-COM	Unsecured data transmission method in B1A
HIGH	1946009	XX-SER-SPD	Front-End Malware can Potentially Harm SAP Installations
HIGH	1942511	EHS-MGM-INC	Missing authorization check in Incident Management
HIGH	1934633	XX-PROJ-FI-CA	Missing authorization check in FI-CA
HIGH	1752717	MFG-LPO	Unauthorized usage of application functionality in MFG-LPO
HIGH	1756472	BC-XI-CON-AFW	Update 2 to Security Note 1723641
HIGH	1896988	BC-TWB-TST-P-PA	Missing Authorization Check in ST05
HIGH	1900200	BC-SRV-ARL	Directory traversal in BC-SRV-ARL
HIGH	1802724	BW-BEX-ET-WJR-RT	Unauthorized modification of displayed content in BW-BEX
HIGH	1906927	AC-INT	Missing authorization check in Accounting BAPIs
HIGH	1931016	BC-DWB-TOO-RTA	Missing authorization check in ABAP Runtime Analysis
HIGH	1852146	BC-WD-UR	Potential information disclosure relating to the Portal
HIGH	1773912	BC-CST-MS	Missing authorization check in message server
HIGH	1862392	PS-MAT-PRO	Missing authorization check in PS-MAT-PRO
HIGH	1776718	BC-JAS-SEC	Missing authorization check in password telnet command
HIGH	1866296	IS-B-BCA-MD	Missing authorization check in IS-B-BCA
HIGH	1782753	BC-MUS-KFM	Missing whitelist check for Key Figure Calculation report
HIGH	1908647	BI-RA-EXP	cross site flashing
HIGH	1908562	BI-RA-EXP	Potential information disclosure relating to SBOP Explorer
HIGH	1909770	FIN-FSCM-COL	Missing whitelist check in SAP Collections Management
HIGH	1909858	CA-GTF-WFM	Missing whitelist check in CA-GTF-WFM

Appendix: SAP Security Notes, December 2013 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	1793359	LO-MD-BP-VM-ES	Missing authorization check in Supplier Entreprise Service
HIGH	1911523	BC-CCM-PRN	Hard-coded credentials in Backend Printing
HIGH	1913554	BC-ESI-BOF	Hard-coded credentials in Suite BOPF
HIGH	1917054	CRM-BTX-GWI	Untrusted XML input parsing possible in CRM-BTX-GWI
HIGH	1925908	CRM-ISA-BBS	Missing authorization check in CRM-ISA-BBS
HIGH	1926485	BC-CCM-MON-SLG	Missing authorization check in application &quot;Edit System Log and Security Audit Log Messages&quot;
HIGH	1927859	BC-SYB-ASE	Missing authentication check in SAP Sybase ASE
MEDIUM	1706769	FS-RI	Missing authorization check in FS-RI
MEDIUM	1956812	SCM-APO-ATP	Update #1 to security note 1425123
MEDIUM	1768656	BC-XI-IBC	PI SEC: Unauthorized modification of displayed content in PI
MEDIUM	1739529	BC-XI-IBF	Potential information disclosure relating to passwords
MEDIUM	1819139	BC-CST-LL	Missing authorization check in SAP Kernel
MEDIUM	1661551	SRM-EBP-CAT	Potential information disclosure relating to SRM-MDM Catalog
MEDIUM	1661781	SRM-CAT-MDM	Potential information disclosure relating to SRM-MDM
MEDIUM	1896642	BC-MID-ALE	Potential information disclosure relating to Integration Technology ALE
MEDIUM	1929338	BC-CCM-SLD-ABA	Potential information disclosure relating to System Landscape Directory ABAP Connectivity
MEDIUM	1785662	SD-BIL-IV-IF	Directory-Traversal in externer Fakturaschnittstelle
MEDIUM	1942432	FI-LA	Missing authorization check in FI-LA
LOW	1831266	BC-XI-IS	Missing authorization check in BC-XI-IS

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.

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.