Layer Seven Security

ADVISORY

SAP Security Notes

May 2015

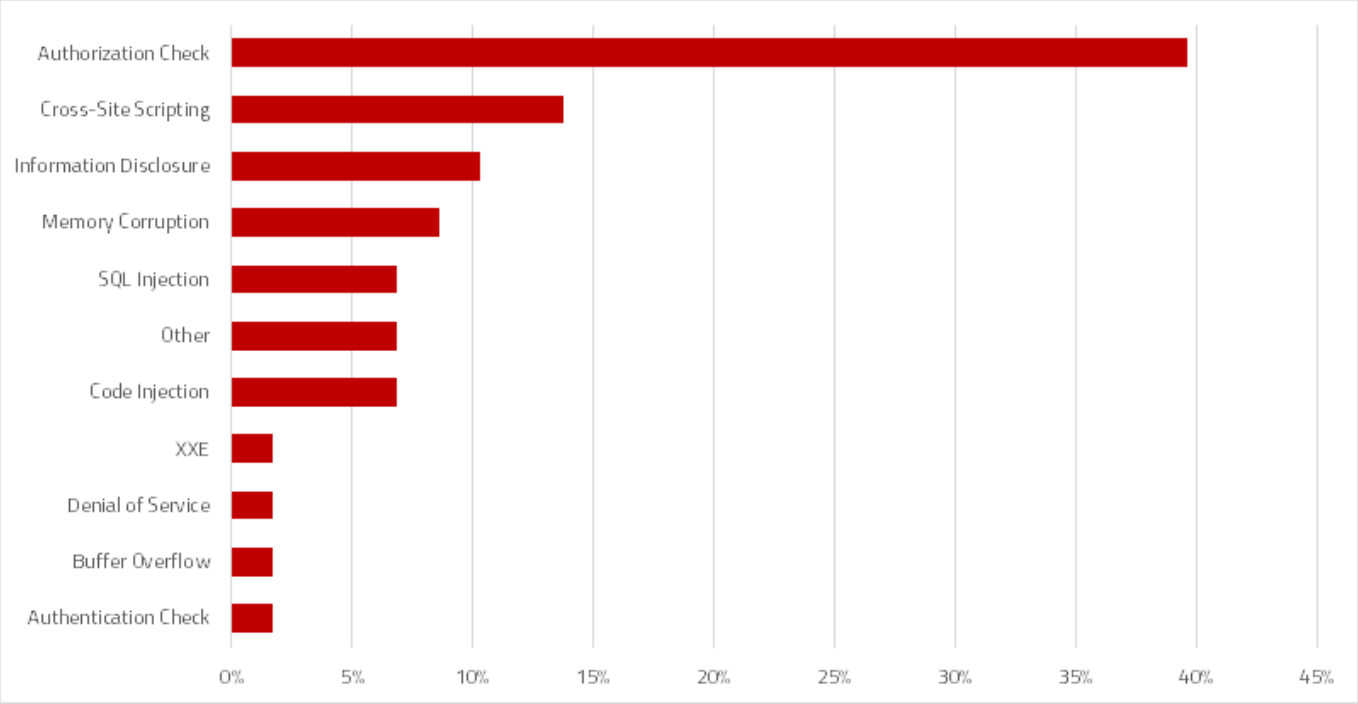
SAP Security Notes

May 2015

SAP released several significant patches in May for memory corruption vulnerabilities effecting multiple applications and components. Such weaknesses can be exploited to provoke a denial of service through conditions that lead applications to attempt to read outside their designated memory space. Notes 2127995, 2125316, 2001108, and 2124806 provide instructions for removing memory corruption flaws in Business Intelligence, Content Server, SAPCAR and SAPGUI, while Note 2121661 provides similar instructions for ABAP and Java server components including the Kernel, R3trans, JCo, SAP.NET and the RFC SDK. Customers can use the Memory Analysis Tool in the ABAP Debugger to analyze memory sizes and other memory-related information for custom, non-SAP delivered programs.

Note 1980992 deals with a high risk privilege escalation vulnerability in the SAP Host Agent that supports database and operating system monitoring, instance control and other critical administrative functions. The vulnerability arises from a race condition or, more specifically, a programming flaw caused by a difference between the Time Of Check and the Time Of Use of access privileges, otherwise known as a TOCTOU software error. The flaw could be exploited by attackers to obtain root access to the local operating system of the Host Agent. Customers should install version 7.20 with SP level 207 or higher to remove the vulnerability.

Note 2067259 fixes an error in report RSUSR003 used to monitor the security of standard users such as SAP*, DDIC and EARLYWATCH including the status of default passwords for delivered users. The implementation of the corrections included



SAP Security Notes by Vulnerability Type

in the Note will lead to the inclusion of the values of the following login-related profile parameters in the header of the report: login/password_downwards_compatibility, login/no_automatic_user_sapstar, and login/password_logon_usergroup. The corrections also add an additional column to the report to correctly display information related to user types.

Finally, Note 2078596 highlights the various enhancements introduced by SAP to strengthen security for Remote Function Calls (RFC). This includes improved guidance via the white paper Securing Remote Function Calls, managing remote access to RFC-enabled Function Modules (FM) using Unified Connectivity (UCON), the introduction of hardcoded authorization checks, and limiting the use of specific FMs to internal scenarios only. Other enhancements include the use of switchable authorization checks for sensitive FMs. The switchable checks delivered by SAP are intended to address known limitations in the use of RFC authorizations such as S_RFC and are listed in Note 2078596.

Appendix: SAP Security Notes, May 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2172204	CA-GTF-DOB	Update 1 to Security Note 1661636
HIGH	1980992	BC-CCM-HAG	Privilege Escalation (root) in hostexecstart
HIGH	2130467	BI-BIP-BIW	Unauthorized modification of displayed content in Performance Management Application
HIGH	2131081	BI-BIP-BIW	Unauthorized modification of displayed content in Performance Management Application
HIGH	2131062	BI-BIP-BIW	Unauthorized modification of displayed content in Performance Management Application
HIGH	2131064	BI-BIP-BIW	Unauthorized modification of displayed content in Performance Management Application
HIGH	1985340	BC-JAS-ADM-ADM	Potential information disclosure relating to NW AS Java
HIGH	2132305	CRM-IM-IPM	Potential modif./disclosure of persisted data in CRM-IM-IPM
HIGH	2137784	GRC-AUD	Missing authorization check in GRC-AUD
HIGH	2138270	BC-BMT-WFM	Missing authorization check in BC-BMT-WFM
HIGH	2125316	BC-INS-TLS	Potential termination of running processes in SAPCAR
HIGH	2155690	MOB-AFA	Missing authentication check in SAP Afaria
HIGH	2155153	BC-SYB-ASE	Potential arbitrary code execution using JAVA in SAP ASE
HIGH	2153690	MOB-AFA	Multiple vulnerabilities in SAP Afaria Server
HIGH	2153898	HAN-WDE	Multiple vulnerabilities have been discovered in HANA Web-based Development Workbench
HIGH	2153892	HAN-WDE	Code injection vulnerability in SAP HANA Web-based Development Workbench
HIGH	2153765	HAN-WDE	Potential modif./disclosure of persisted data in SAP HANA Web-based Development Workbench
HIGH	2152278	BC-SYB-ASE	Multiple vulnerabilities in SAP ASE.
HIGH	2001108	BI-BIP-AUT	Potential remote termination of running processes in BI-BIP
HIGH	2090851	BC-CCM-SLD-JAV	Untrusted XML input parsing possible in SLD
HIGH	2085588	SV-SMG-SDD	Code injection vulnerability in SV-SMG-SDD
MEDIUM	1952094	XX-CSC-AR-FI	Missing authorization check in XX-CSC-AR-FI
MEDIUM	2166849	BC-JAS-SEC-LGN	Update 1 to Security Note 2079002
MEDIUM	2067259	BC-SEC-USR-IS	RSUSR003 Wrong Password Status
MEDIUM	2055083	BC-XI-IS-IEN	Potential information disclosure relating to BC-XI-IS-IEN
MEDIUM	2030377	IS-B-BCA	Missing authorization check in IS-B-BCA
MEDIUM	2029397	CRM-ISA-R3	Missing authorization checks for RFC in E-commerce ERP applications

Appendix: SAP Security Notes, May 2015 Cont.

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2127995	BC-SRV-KPR-CS	Potential remote termination of running processes in Content Server
MEDIUM	2131065	BI-BIP-BIW	Unauthorized modification of displayed content in Performance Management Application
MEDIUM	2131334	BC-SRV-PMI	Missing authorization check in Process Monitoring Infrastructure
MEDIUM	2105634	BC-MID-ALE	Missing authorization check in ALE Interface
MEDIUM	2105620	BC-SRV-GBT-CAL	Missing authorization check in Calendar Interface
MEDIUM	2053788	BC-MOB-MI-SER	Missing authorization check in RFC enabled function module - BC-MOB-MI-SER
MEDIUM	2105633	BC-SRV-GBT-ALM	Missing authorization check in Alert Management Interface
MEDIUM	2138031	BC-BMT-WFM	Missing authorization check in BC-BMT-WFM
MEDIUM	2138219	BC-BMT-WFM	Missing authorization check in BC-BMT-WFM
MEDIUM	2052677	BC-TWB-TST-ECA	Possible code injection and missing RFC authentication
MEDIUM	2053043	BC-TWB-TST-ECA	Missing RFC authorization in eCATT Extended Computer Aided Test Tool
MEDIUM	2152230	PY-US-RP	Switchable authorization checks for RFC in Reconciliation Report Scheduler
MEDIUM	2149278	BC-SRV-RM	Missing authorization check in SAP Records Management
MEDIUM	2143329	BC-CTS-ORG-PLS	Missing authorization check in RDDPUTJZ_COPY_TRANSPORT
MEDIUM	2140238	BC-XI-IS-BPE	Missing authorization check in BC-XI-IS-BPE
MEDIUM	2124806	BC-FES-GUI	Potential remote termination of running processes in SAP GUI
MEDIUM	2122840	BC-FES-AIT-CTR	Error with user verification when Logon Control is used.
MEDIUM	2121661	BC-MID-RFC	Potential remote termination of running processes in ABAP & Java Server
MEDIUM	2121461	BC-FES-CON	Potential information disclosure relating to SAPConsole
MEDIUM	2118500	BC-SRV-RM	Missing authorization check in SAP Records Management
MEDIUM	2078596	BC-MID-RFC	Further improvements for RFC security
MEDIUM	2072357	SRM-EBP-CA-ACC	Switchable authorization checks for RFC in SRM application.
MEDIUM	2067630	BC-DB-DB6-CCM	DBA Cockpit: Missing authorizations during administration of jobs and scripts
MEDIUM	2066943	WEC-APP-UM	New authorization check for RFC in component WEC-APP-UM
MEDIUM	2066851	BC-UPG-OCS	Missing authority-check vulnerability in the OCS functionality (Support Package Manager / Add-On Installation Tool)
MEDIUM	2150625	LO-SLC	Potential disclosure of persisted data in SAP CPQ Solution Sales Configuration
LOW	2058351	BC-VMC	Missing authorization check in BC-VMC

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