ADVISORY

Layer Seven Security

SAP Security Notes

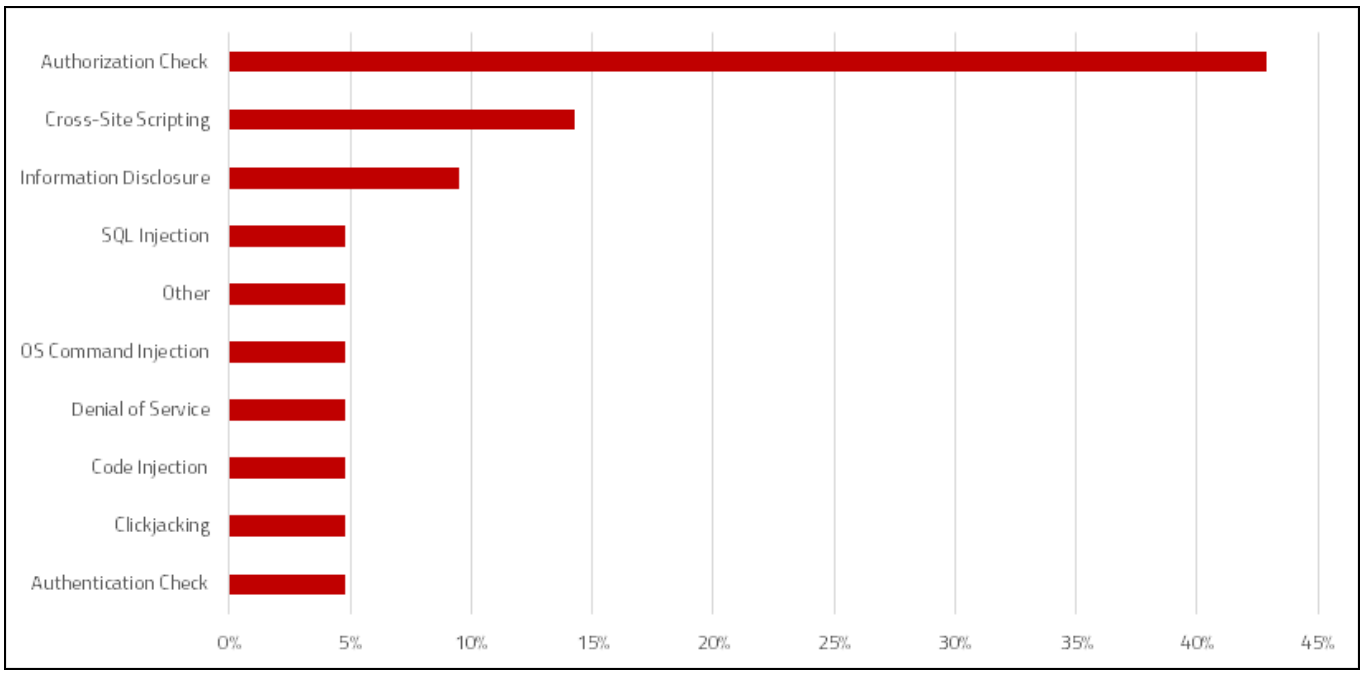
November 2016

SAP Security Notes

November 2016

Hot News Note 2357141 addresses a critical OS command injection vulnerability in the terminology export report program of SAPterm (transaction STERM). STERM is used to search SAP-delivered terminology and create and maintain customer-specific terminology. TERM_EXCEL_EXPORT is a standard executable program that enables users to export terminology repositories to Excel. The program calls function modules that accept unfiltered user commands in expressions that are used to call systems. This could be abused by attackers perform arbitrary operating system commands using the elevated privileges of the <sid>adm user. The impact of such an exploit could include compromise of the entire SAP file system in the effected host. This explains the high CVSS base score of 9.1 / 10 for Note 23557141. The Note rates high in terms of the impact to information confidentiality, integrity and availability. Systems with SAP_BASIS versions 7.31 – 7.66 should be patched to the relevant Support Package level listed in the Note.

Note 2371726 deals with a similar OS command injection vulnerability in Text Conversion, an application that enables users to replace standard text with customer-specific text through the function module BRAN_DIR_CREATE. The Note carries the identical CVSS score to Note 2357141 and impacts systems with SAP_BASIS versions 7.00 – 7.51. The corrections should be applied after the implementation of the prerequisite Note 1673713.



SAP Security Notes by Vulnerability Type

Note 2366512 removes a dangerous information disclosure vulnerability in the SAP Software Update Manager (SUM). SUM is used for system maintenance including managing upgrades, installing enhancement packs, and applying support packages. SUM should be upgraded to SP017, patch level 10 to prevent the storage of the credentials for the MSSQL database shadowuser in plain-text log files.

Finally, Note 2358972 provides a kernel patch to block Distributed Denial of Service (DDOS) attacks provoked by requests that lead to resource exhaustion in the message server. The availability of SAP services could be interrupted by attacks that crash or flood the message server.

Appendix: SAP Security Notes, November 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2357141	BC-DOC-TER	OS Command Injection vulnerability in Report for Terminology Export
HOT NEWS	2371726	BC-DOC-RIT	Code Injection vulnerability in Text Conversion
HIGH	1718613	BC-UPG-TLS-TLA	Missing authorization check in FM DD_DB_IMIG_CALL_INSTTOOL
HIGH	2101079	BC-ESI-UDDI	Potential modif./disclosure of persisted data in BC-ESI-UDDI
HIGH	2358972	BC-CST-MS	Denial of service (DOS) in Message Server
HIGH	2366512	BC-DB-MSS	Information Disclosure in SAP Software Update Manager
MEDIUM	2245130	BC-MID-RFC	Potential bypass of unified connectivity runtime checks possible in BC-MID-RFC
MEDIUM	2378485	CRM-MKT-MPL-CAL	Cross-Site Scripting (XSS) vulnerability in Integrated Marketing Calendar
MEDIUM	2142551	BC-WD-ABA	Whitelist service for Clickjacking Framing Protection in AS ABAP
MEDIUM	2248862	FI-CAX-INV	Missing authorization check in FI-CA-INV
MEDIUM	1434761	BC-XI-IBC	Storing passwords of XI/PI service users
MEDIUM	2368873	FS-AM-OM-SO	Missing Authorization check in Banking Services / Standing Order
MEDIUM	2367193	XX-CSC-RU-FI	Missing Authorization check in Cash Flow Statement report
MEDIUM	2342940	BC-CCM-SLD	Information Disclosure in System Landscape Directory
MEDIUM	2371610	FI-GL-GL-J	Missing Authorization check in Direct-Input posting
MEDIUM	2368106	EPM-BFC-TCL	Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Financial Consolidation
MEDIUM	2366726	BC-XI-IS-IEN	Cross-Site Scripting (XSS) vulnerability in PI Integration Engine
MEDIUM	2383912	CA-WUI-APF	Insecure Logoff functionality in CA-WUI-APF
MEDIUM	2263882	CRM-MD-INB	Missing authorization check in CRM-MD-INB
LOW	2250863	XX-CSC-IN-MM	Missing authorization check in XX-CSC-IN-MM
LOW	2376223	BC-DWB-UTL	Missing Authorization check in Dynpro Modeler

LAYER SEVEN SECURITY

Layer Seven Security empowers organizations 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

555 Industrial Drive
Suite 107
Milton, Ontario
L9T 5E1, Canada

Web

www.layersevensecurity.com

Email

info@layersevensecurity.com

Telephone

1-647-964-7370

SAP Partner