ADVISORY

Layer Seven Security

SAP Security Notes

October 2017

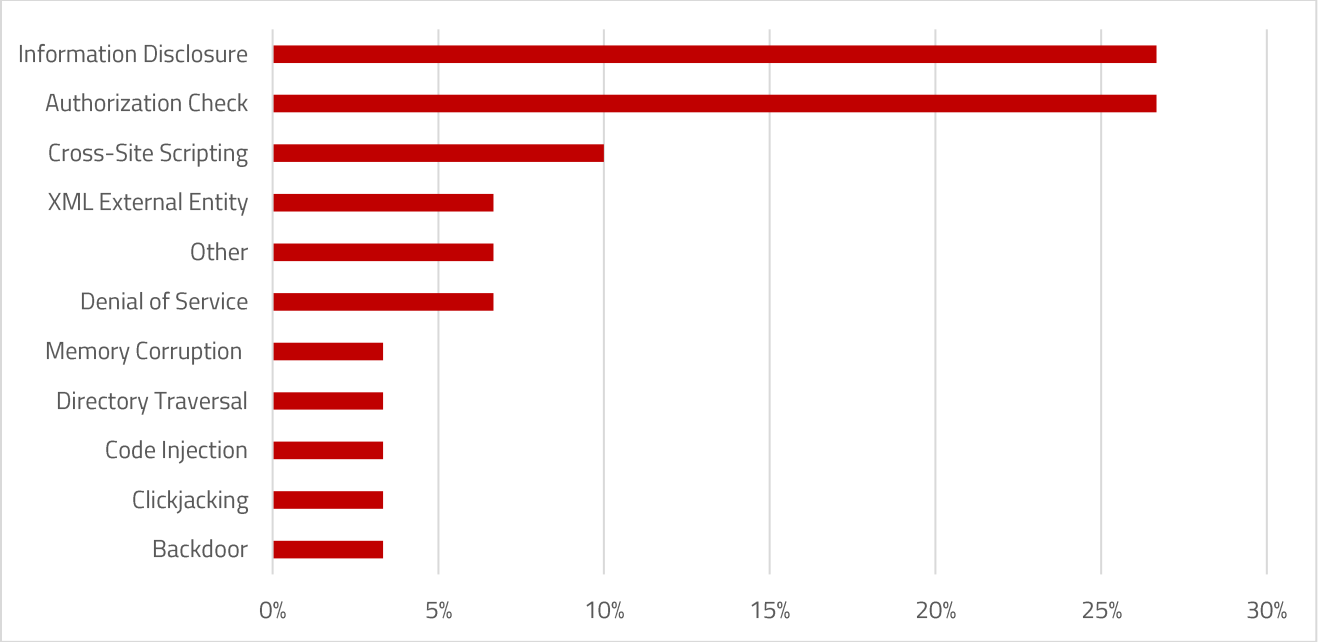
SAP Security Notes

October 2017

SAP issued an important update for Hot News Note 2371726 originally released in November 2016. The note addresses a code injection vulnerability in Text Conversion which enables SAP standard text to be replaced by industry specific text. Function module BRAN_DIR_CREATE in Text Conversion enables an authenticated development user to inject operating system commands and execute these from the SAP system via that function. Developer rights through the S_DEVELOP authorization object are required for the successful execution of the exploit. Nonetheless, the note carries a CVSS score of 9.10/ 10 and rates high in terms of impact to data confidentiality, integrity and availability. The note includes corrections for SAP Basis versions 700 – 751 which restrict the range of supported special characters and the directory created by function module BRAN_DIR_ CREATE.

Note 2486657 patches a high-risk directory traversal vulnerability in the API Engine of AS Java which arises from insufficient path validation performed by the Servlet API for resource requests. This could lead attackers to read the content of arbitrary files on servers and expose sensitive data to corruption or deletion. The Note includes instructions for updating versions 7.10 – 7.50 of AS Java to the latest patch level including the vulnerable components ENGINEAPI, J2EE ENGINE, J2EE ENGINE CORE and JEECOR.

Note 2476937 delivers a patch for a critical denial of service vulnerability in the SAP



SAP Security Notes by Vulnerability Type

Standalone Enqueue Server which is used to support direct TCP connections between clients and servers that bypass dispatchers and message servers. Attackers can trigger resource exhaustion in the Server using specific requests. The Note includes kernel patches for SAP Kernel versions 7.21 – 7.53.

Note 2408073 includes updated instructions for manual activities required to prepare SAP systems to process digitally signed Notes. The note also includes sample files to test the security features once they are enabled.

Appendix: SAP Security Notes, October 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2371726	BC-DOC-RIT	Code Injection vulnerability in Text Conversion
HIGH	2486657	BC-JAS-WEB	Directory Traversal vulnerability in SAP NetWeaver AS Java Web Container
HIGH	2476937	BC-CST-EQ	Potential Denial of Service vulnerability in SAP Standalone Enqueue Server
MEDIUM	2492658	EP-BC-UWL	Missing XML Validation vulnerability in SAP NetWeaver Java Workflow (JWF)
MEDIUM	2503107	PM-WOC-MO	Missing authorization checks in PM-WOC-MO
MEDIUM	2319174	BC-FES-BUS-HTM	Whitelist based Clickjacking Framing Protection in NWBC for HTML
MEDIUM	2408073	BC-UPG-NA	Handling of Digitally Signed notes in SAP Note Assistant
MEDIUM	2491578	FS-CML	Fehlende BerechtigungsprÃ¼fung in der Darlehensverwaltung
MEDIUM	2471209	BC-FES-ITS	Cross-Site Scripting (XSS) vulnerability in SAPGUI for HTML
MEDIUM	2458021	BI-BIP-AUT	Information Disclosure vulnerability in LDAP Authentication for SAP BusinessObjects Enterprise
MEDIUM	2527770	BC-CCM-SLD-JAV	Information Disclosure in SAP NetWeaver System Landscape Directory
MEDIUM	2236258	XX-PART-ADB-IFM	Missing XML Validation vulnerability in Adobe Document Services
MEDIUM	2511453	MOB-SDK-MAF	Possible leakage of sensitive data in SAP Mobile Platform SDK 3.0
MEDIUM	2517501	IS-PS-CA	Switchable Authorization checks for SAP ERP Funds Management Account Assignments
MEDIUM	2480857	BC-WD-ABA-RUN	Denial of Service in SAP NetWeaver Web Dynpro ABAP
MEDIUM	2519135	CRM-MKT-ML	Cross-Site Scripting (XSS) vulnerability in SAP CRM Mail Form Editor
MEDIUM	2519622	CRM-IC-CHA-EMA	Email Spoofing vulnerability in SAP CRM IC WebClient
MEDIUM	2509284	BC-CST-STS	Memory Corruption vulnerability in SAP NetWeaver Instance Agent Service
MEDIUM	2504129	BC-CST-STS	Information Disclosure in SAP NetWeaver Instance Agent Service
MEDIUM	2264949	CRM-MW-GEN	Switchable authorization checks for RFC in CRM-MW-GEN

Appendix: SAP Security Notes, October 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2264948	CRM-MW-SRV	Switchable authorization checks for RFC in CRM-MW-SRV
MEDIUM	2457014	PA-PA-US	Missing Authorization check in PA-PA-US
MEDIUM	2314976	BC-JAS-WEB	Content spoofing in AS Java Web container
MEDIUM	2479448	PY-US-TP	Missing Authorization check in PY-US-TP
MEDIUM	2457929	PY-US	Missing Authorization check in PY-US
LOW	2353643	BC-WD-ABA	Information Disclosure in Webdynpro LIST UIBB: Search hits are marked in invisible cells
LOW	2532802	BC-MOB-LAP	Information Disclosure in SAP NetWeaver Mobile Client
LOW	2528284	BC-MOB-LAP	Information Disclosure in SAP NetWeaver Mobile Client
LOW	2510269	BC-MOB-LAP	Information disclosure vulnerability in SAP NetWeaver Mobile Client
LOW	2528596	IS-R-TGM-POS	Hard-coded Credentials in SAP Point of Sale Store Manager

LAYER SEVEN SECURITY

Layer Seven Security serve customers worldwide to harden, patch and monitor SAP systems against cyber threats using SAP Solution Manager

Address

99 Hudson Street
5th Floor
New York, NY 10013
United States

Web

www.layersevensecurity.com

Email

info@layersevensecurity.com

Telephone

1-647-964-7370