ADVISORY

Layer Seven Security

SAP Security Notes

June 2017

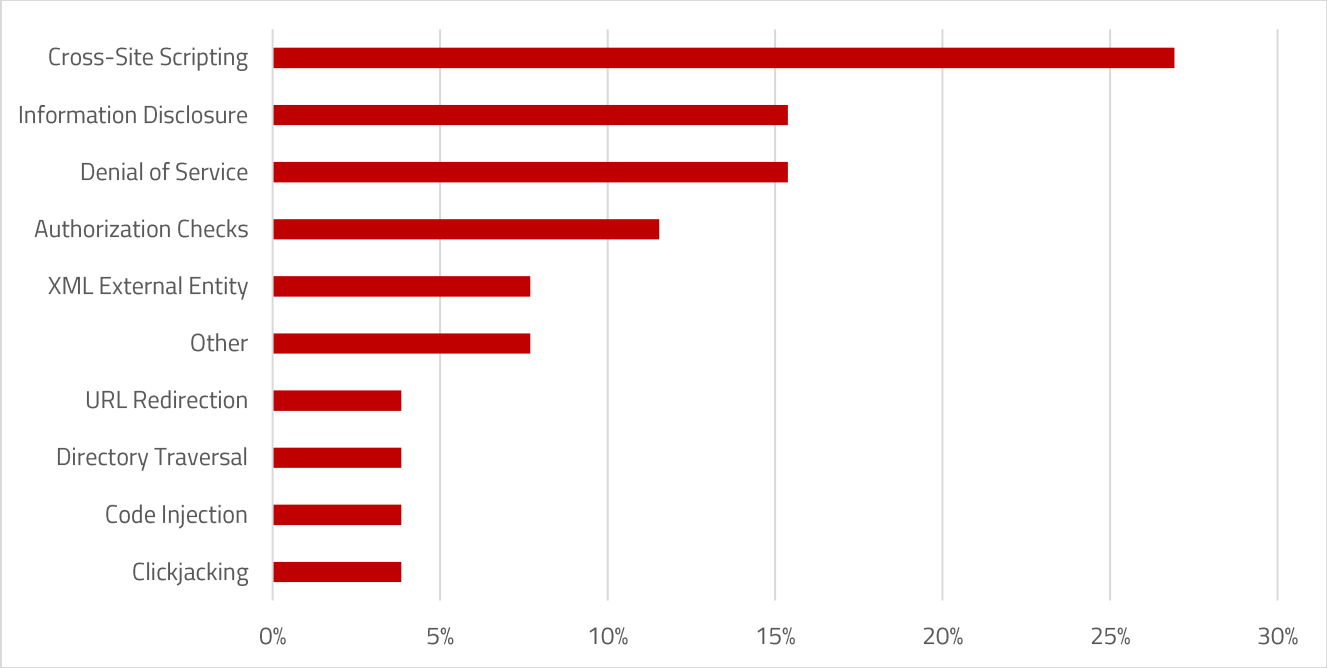
SAP Security Notes

June 2017

Note 2416119 was reissued in June with updated release information and solution instructions. The note provides instructions for maintaining the property URLCheck ServerCertificate in Java Application Servers. The instructions are intended to mitigate the risk of man-in-the-middle attacks by securing client-server HTTPS connections. Certificates signed by Certificate Authorities should be maintained in client keystores to avoid possible failures in HTTPS calls. Detailed instructions are available in the Manual Activities section of Note 2416119 and in the Resolution section of Note 2452615.

Note 2444321 corrects a program error in the SsfVerifyEx function of the SAP Common Cryptographic Library (Common CryptoLib). The error can lead to a failure in authorization and authentication checks for certificates. SAP-delivered applications do not use the vulnerable SsfVerifyEx function. However, SsfVerifyEx may be called by custom programs through the function module SSFW_KRN_VERIFY within the SSFW function group and the method VERIFY_XML within the SAP class CL_SEC_SXML_DSIGNATURE.

Notes 2313631 and 2389181 deal with Denial of Service vulnerabilities impacting the Launchpad and Central Management Console (CMC) within Business Intelligence and the Instance Agent Service (sapstartsrv), respectively. The Launchpad and CMC are popular portals used to access BI content.



SAP Security Notes by Vulnerability Type

Sapstartsrv is a host-level service for controlling and monitoring SAP processes.

Note 2427292 includes corrections for an information disclosure vulnerability in the Microsoft Management Console (MMC) that could enable attackers to discover the password of hidden users. The credentials could be used to start or stop Java systems via the MMC Web Service.

Appendix: SAP Security Notes, June 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2416119	BC-JAS-WEB	Improved security for outgoing HTTPS connections in SAP NetWeaver
HIGH	1854252	BC-SRV-ALV	Missing authorization-check in BC-SRV-ALV
HIGH	2313631	BI-BIP-INV	Denial of service (DOS) in BILaunchPad and Central Management Console
HIGH	2444321	BC-IAM-SSO-CCL	Missing certificate verification in CommonCryptoLib
HIGH	2396544	BI-RA-WBI-FE-HTM	Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Web Intelligence HTML interface
HIGH	2389181	BC-CST-STS	Denial of service (DOS) in SAP NetWeaver Instance Agent Service
MEDIUM	2389764	BW-BEX-OT-WSP	BW Workspaces: Analysis authorization during modeling and running local hierarchies
MEDIUM	2142551	BC-WD-ABA	Whitelist service for Clickjacking Framing Protection in AS ABAP
MEDIUM	2253026	IS-U-CA	Fehlende BerechtigungsprÃ¼fung in IS-U-CA
MEDIUM	2422292	EPM-BFC-PSI-INS	Cross-Site Scripting (XSS) vulnerability in SAP Business Objects Financial Consolidation
MEDIUM	2425129	BC-UPG-NA	Missing XML Validation vulnerability in SAP Note Assistant
MEDIUM	2457269	EPM-BPC-NW-AR	Missing XML Validation vulnerability in Business Planning & Consolidation system reports
MEDIUM	2445071	BC-CST-MS	Denial of service (DOS) in SAP NetWeaver Message Server
MEDIUM	2430022	BC-CST	Denial of service (DOS) in SAP Netweaver AS ABAP
MEDIUM	2445033	BC-CST-MS	Information Disclosure in SAP NetWeaver Message Server

Appendix: SAP Security Notes, June 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2405943	BC-DWB-JAV-CAF	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Composite Application Framework and Business Warehouse Test Integration
MEDIUM	2472026	EIM-DS-SVR	URL Redirection vulnerability in SAP Data Services Management Console
MEDIUM	2457909	SCM-FRE-ERP	Missing Authorization check in SCM Forecasting and Replenishment
MEDIUM	2429693	EPM-IC-PSI	Directory Traversal vulnerability in SAP BusinessObjects Intercompany 10.0
MEDIUM	2427292	BC-JAS-SF	Information disclosure in SAP MMC Console
MEDIUM	2423429	BC-CST-WDP	Code Injection vulnerability in SAP Web Dispatcher
MEDIUM	2419559	BI-RA-WBI-FE-HTM	Reflected Cross-Site Scripting (XSS) in Web Intelligence BI Launchpad
MEDIUM	2419524	BI-RA-WBI-FE-HTM	Reflected Cross-Site Scripting (XSS) in Web Intelligence BI Launchpad
MEDIUM	2189781	BC-FES-BUS-HTM	Unauthorized modification of displayed content in NWBC for HTML
MEDIUM	2373032	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in WebClient User Interface
MEDIUM	1816886	EHS-MGM-INC	Potential information disclosure in investigation

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