LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

February 2019

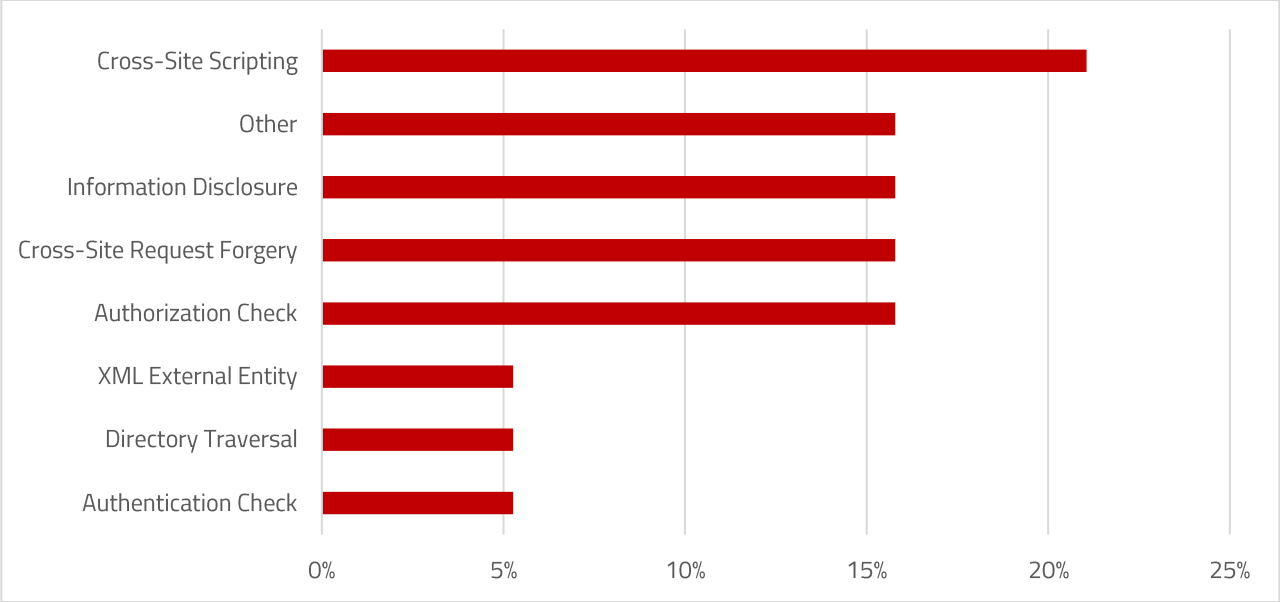
SAP Security Notes

February 2019

Hot News Note 2742027 patches a critical broken authentication check in SAP HANA Extended Application Services, advanced model. The vulnerability could lead to unauthorized administrative access and the exfiltration, modification or deletion of sensitive data in HANA XS. The vulnerability carries a CVSS score of 9.4/10. It ranks relatively low in terms of attack complexity and requires no privileges in target systems. HANA XS Advanced should be upgraded to the patch level specified in the Note to address the risk. The Note includes manual instructions for a workaround if an upgrade is not possible. The workaround removes the affected OIDC component. A side-effect of the workaround is the deactivation of X.509-based or SPNEGO single sign-on for HANA users.

Note 2070691 deals with a high priority information disclosure vulnerability in the SAP Solution Tools Plug-In (ST-PI) that could lead to the leakage of sensitive data including configuration data and user passwords. The information can be used to perform targeted attack against database servers for SAP systems.

Note 2729710 includes a correction for a missing XML Validation vulnerability in the System Landscape Directory (SLD).



SAP Security Notes by Vulnerability Type

The correction avoids processing of all XML files that use XML External Entity (XXE). This could cause the SLD to continuously loop, read arbitrary files and send local files.

Appendix: SAP Security Notes, February 2019

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for the browser control Chromium delivered with SAP Business Client
HOT NEWS	2742027	BC-XS-SEC	[CVE-2019-0261] Missing authentication check in SAP HANA Extended Application Services, advanced model
HIGH	2070691	SV-SMG-SDD	Potential information disclosure relating to database server file system
HIGH	2729710	BC-CCM-SLD-REG	[CVE-2019-0265] XML External Entity (XXE) vulnerability in SLD Registration of ABAP Platform
HIGH	2724014	EPM-DSM-GEN	[CVE-2019-0258] Missing Authorization check in SAP Disclosure Management
HIGH	2723570	BC-ABA-SC	[CVE-2019-0255] ABAP Platform provides access to Easy Access Menu
MEDIUM	2733972	BW-BEX-OT-BICS-INA	Cross-Site Request Forgery (CSRF) vulnerability in BICS InA Interface
MEDIUM	2662687	IS-B-BCA-MD	[CVE-2018-2484] Missing Authorization check in SAP Enterprise Financial Services
MEDIUM	2638175	BI-BIP-INV	[CVE-2019-0251] Cross-Site Scripting (XSS) vulnerability in SAP Business Objects Fiori Launchpad
MEDIUM	2706798	EPM-DSM-GEN	[CVE-2019-0254] Cross-Site Scripting (XSS) vulnerability in SAP Disclosure Management
MEDIUM	1827555	SRM-EBP-CA-UI	Cross-Site Scripting (XSS) vulnerability in SAP SRM
MEDIUM	2728839	BC-CUS-TOL-IMG	[CVE-2019-0257] Missing Authorization check in ABAP Platform
MEDIUM	2727564	BI-BIP-VD	[CVE-2019-0259] Unrestricted File Upload vulnerability in BO 4.2/ Visual Difference
MEDIUM	2724713	BC-XS-RT	[CVE-2019-0266] Potential Information Disclosure in SAP HANA Extended Application Services, Advanced Model
MEDIUM	2723878	SBO-MOB-APP	[CVE-2019-0256] Information Disclosure in SAP Business One Mobile app for Android

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2711074	FI-LOC-SRF-DEF	Cross-Site Request Forgery (CSRF) vulnerability in SAP S/4 HANA for Advanced Compliance Reporting/ Define Advanced Compliance Report
MEDIUM	2709897	BC-EAD	Directory Traversal vulnerability in SAP Enterprise Architecture Designer v1.0 SP04
MEDIUM	2696714	BI-RA-WBI-SDK	[CVE-2019-0262] Cross-Site Scripting (XSS) vulnerability in Web Intelligence BI Launch Pad
MEDIUM	2686535	MFG-MII	[CVE-2019-0267] Cross site request forgery in implementation of Manufacturing Integration and Intelligence

LAYER SEVEN SECURITY

Layer Seven Security secure, patch and monitor SAP systems against cyber threats using SAP Solution Manager. Layer Seven's innovative and patent-pending Cybersecurity Extension for Solution Manager extends the capabilities of Solution Manager for advanced vulnerability management, threat detection and incident response.

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

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.