LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

September 2018

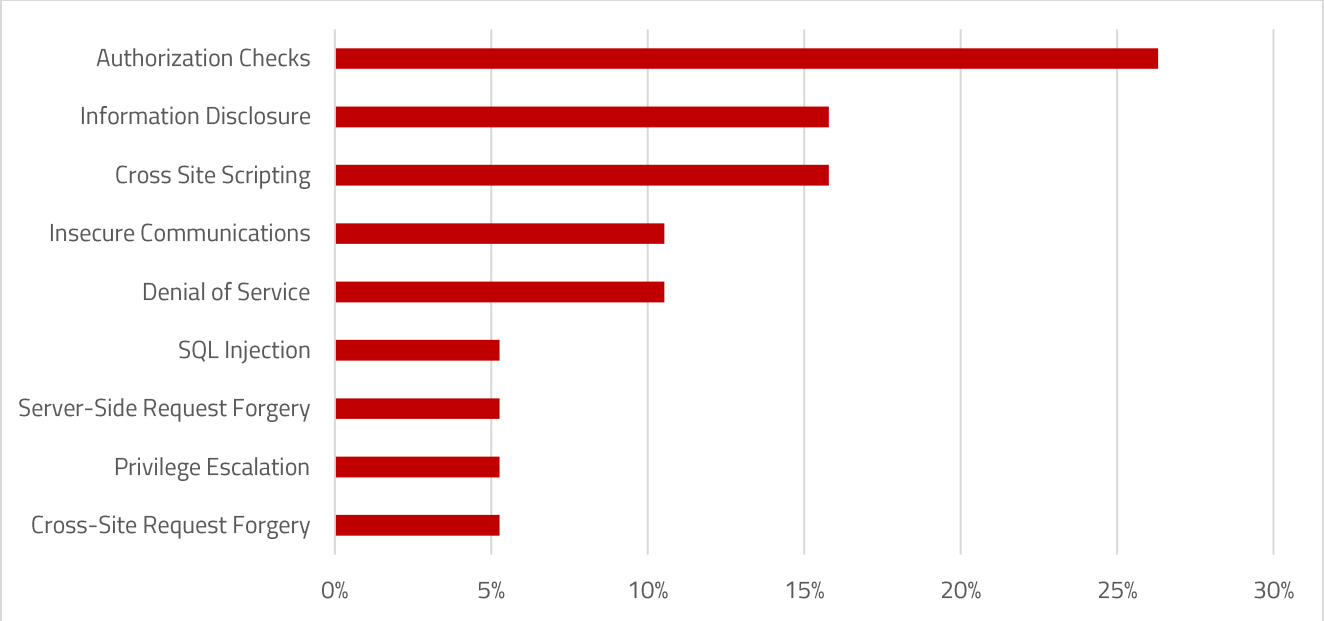
SAP Security Notes

September 2018

Note 2681207 patches a high-risk missing XML validation vulnerability in Extended Application Services (XS) in SAP HANA. The OData parser in HANA XS does not sufficiently validate XML input from users. This can lead to the processing of malicious code that could provoke a denial of service in the database server. The vulnerability can be exploited if applications using OData services are enabled on HANA XS. If authentication is not enforced for an enabled application using OData, an anonymous attacker can exploit the vulnerability. The attacker needs network access to the HTTP/HTTPs port of the SAP HANA database XS engine classic model. The vulnerability can be fixed by applying the software packages listed in note 2681207. Alternatively, you can limit network access to the XS classic server running in the tenant databases of a multitenant system. The default port range is 30040 – 30997. It is also recommended to enforce authentication for applications using OData services via HANA XS.

Note 2644279 deals with a similar high-risk missing XML validation vulnerability in a component of the BEx Web Java Runtime in Business Warehouse. The issue is specific to PDF ALV Export.

Note 2392860 removes transaction ZPTTNO_TIME from the standard roles SAP_PS_RM_PRO_ADMIN and SAP_PS_RM_PRO_REVIEWER in SAP CRM Case Management. The transaction could be abused to escalate privileges.



SAP Security Notes by Vulnerability Type

Other high priority notes include note 2670284 which updates logging functions in Crystal Reports and Business One for HANA to prevent the disclosure of sensitive information, and note 2449974 which introduces authorization check V_VBKA_VKO for specific Sales Support APIs in ECC Sales and Distribution.

Appendix: SAP Security Notes, September 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2681207	HAN-AS-XS	[CVE-2018-2465] Missing XML Validation vulnerability in SAP HANA, Extended Application Services classic model
HIGH	2392860	BC-SRV-RM	Leveraging privileges by customer transaction code
HIGH	2670284	SBO-CRO-SEC	[CVE-2018-2458] Information Disclosure in SAP Business One
HIGH	2644279	BW-BEX-ET-WJR-EXP	[CVE-2018-2462] Missing XML Validation vulnerability in BEx Web Java Runtime Export Web Service
HIGH	2449974	SD-CAS-SA	Missing Authorization check in SAP ECC Sales Support
MEDIUM	2469377	FIN-TMF-BR-CIAP	Missing Authorization check in CIAP
MEDIUM	2668681	CO-FIO	Cross-Site Request Forgery (CSRF) SAP vulnerability in Manage Profit Centers
MEDIUM	2383017	BC-FES-CTL	Cross-Site Scripting (XSS) vulnerability in SAP GUI HTML Control
MEDIUM	2680834	CEC-COM-CPS	[CVE-2018-2463] Server-Side Request Forgery (SSRF) in SAP Hybris Commerce
MEDIUM	2679788	BC-SYB-ASE	[CVE-2018-2457] Information Disclosure in SAP Adaptive Server Enterprise
MEDIUM	2679378	BC-WD-JAV	[CVE-2018-2464] Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver WebDynpro Java
MEDIUM	2677002	SV-SMG-INS-CFG-MNG	Improper password handling in SAP Solution Manager
MEDIUM	2673959	PA-FIO-PRO	[CVE-2018-2461] Missing authorization check in SAP HCM Fiori app "People Profile"
MEDIUM	2672919	MOB-ONP-OOD	[CVE-2018-2459] Information disclosure in SAP Mobile Platform server Offline OData
MEDIUM	2646067	IS-B-BCA-MD	[CVE-2018-2455] Missing Authorization check in SAP Enterprise Financial Services
MEDIUM	2645133	IS-B-BCA-AM	[CVE-2018-2454] Missing Authorization check in SAP Enterprise Financial Services
MEDIUM	2623846	BC-JAS-SEC-LGN	[CVE-2018-2452] Cross Site Scripting in NW AS Java Logon Application
LOW	2331141	XX-CSC-RU	SQL Injection vulnerability in SAP CIS Country Localization XML Generator
LOW	2682503	SBO-CRO-SEC	[CVE-2018-2460] Insecure certificate verification in SAP Business One Android application

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