LAYER SEVEN SECURITY

ADVISORY

# SAP Security Notes

March 2019

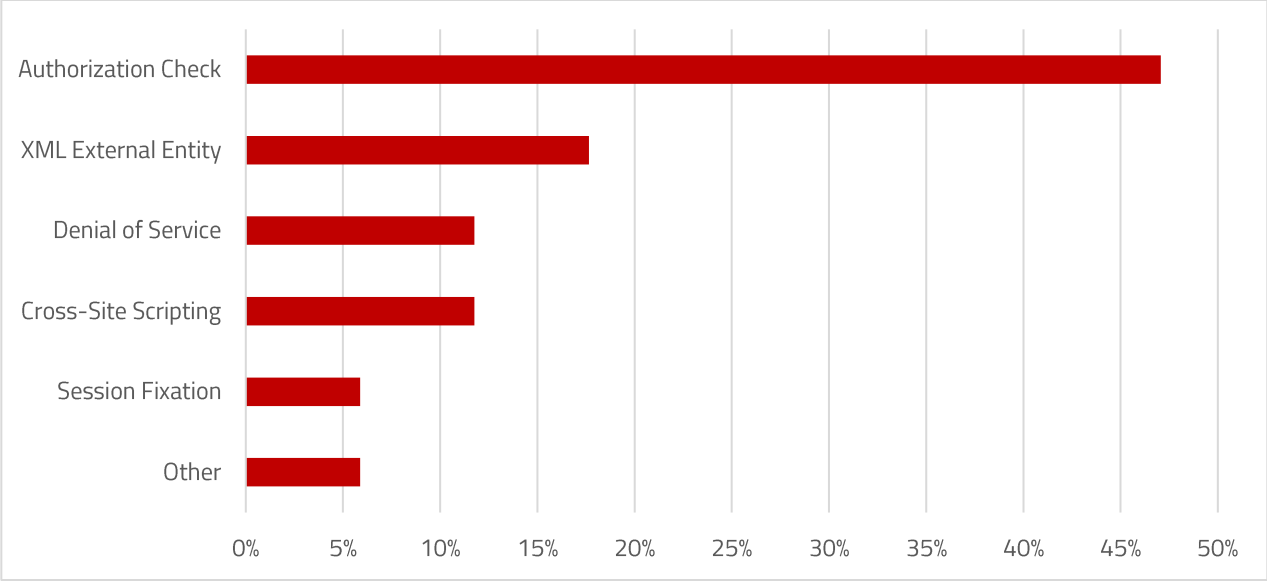
# SAP Security Notes

March 2019

Note 2764283 addresses an XML External Entity vulnerability in SAP HANA extended application services (XS), advanced. HANA XS does not sufficiently validate an XML document accepted from an authenticated developer with privileges to the SAP space. Successful exploitation of the vulnerability could lead to the leading of arbitrary files in SAP servers or denial of service through resource exhaustion. Note that exploits targeting the vulnerability require either administrative or developer privileges to the SAP space of the XS advanced service. SAP recommends updating to XS advanced runtime version 1.0.102 or later.

Note 2689925 deals with a Cross-Site Scripting (XSS) Vulnerability in the SAML 1.1 SSO Demo App in the SAP NetWeaver Application Server Java. The app does not does sufficiently encode user-controlled inputs. This could lead to unauthorized changes to web content and the theft of user credentials. The vulnerability impacts versions 7.10 – 7.50 of the software component J2EE-APPS. SAP recommends upgrading the component to the relevant patch level for each version specified in Note 2689925.

Note 2524203 introduces a switchable authorization check to secure access to the function module FKK_DOCUMENT_READ used to read documents in Accounts Receivable and Payable.




SAP Security Notes by Vulnerability Type

Notes 2662687, 2727689, 2754235, 2746946, 2652102 and 2250863 patch insufficient or missing authorization checks in areas such as SAP Enterprise Financial Services, NetWeaver Application Server ABAP, S/4HANA, Convergent Invoicing and the Payment Engine.

# Appendix: SAP Security Notes, March 2019

| PRIORITY | NOTE | AREA | DESCRIPTION |
|---|---|---|---|
| HIGH | 2764283 | BC-XS-RT | [CVE-2019-0277] XML External Entity vulnerability in SAP HANA extended application services, advanced |
| HIGH | 2689925 | BC-JAS-SEC-LGN | [CVE-2019-0275] Cross-Site Scripting (XSS) Vulnerability in SAP NW SAML 1.1 SSO Demo App |
| MEDIUM | 2662687 | IS-B-BCA-MD | [CVE-2018-2484] Missing Authorization check in SAP Enterprise Financial Services |
| MEDIUM | 2524203 | FI-CA | Switchable authorization checks for RFC in SAP ERP Contract Accounts Receivable and Payable |
| MEDIUM | 2729710 | BC-CCM-SLD-REG | [CVE-2019-0265] XML External Entity (XXE) vulnerability in SLD Registration of ABAP Platform |
| MEDIUM | 2732527 | MFG-PCO | Potential Oracle attack on OPC UA server in SAP Plant Connectivity |
| MEDIUM | 2727689 | BC-ABA-SC | [CVE-2019-0270] Missing Authorization check in ABAP Server of SAP NetWeaver |
| MEDIUM | 2754235 | FS-FPS-SLA | [CVE-2019-0276] Inadequate Authorization check in Banking services from SAP and SAP S/4HANA Financial Products Subledger |
| MEDIUM | 2753497 | MOB-SDK-AGC | [CVE-2019-0274] Denial of service (DOS) in SAP Work and Inventory Manager |
| MEDIUM | 2746946 | FI-CA-INV-FIO | Missing Authorization check in SAP Convergent Invoicing |
| MEDIUM | 2736825 | BC-ABA-XML | [CVE-2019-0271] Denial of Service via XML External Entity (XXE) vulnerability in ABAP Server |
| MEDIUM | 2693962 | BI-BIP-BIW | [CVE-2019-0269] Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects BIWorkspace |
| MEDIUM | 2689259 | BI-BIP-CMC | [CVE-2019-0268] Missing XML Validation vulnerability in SAP BusinessObjects BI Platform CMC module |
| MEDIUM | 2652102 | FS-PE | Missing Authorization checks for Templates and Business Partner Search in Payment Engine |
| MEDIUM | 2030144 | IS-HER-CM | Switchable authorization checks for RFC in SLCM (Student Life cycle Management) |

| PRIORITY | NOTE | AREA | DESCRIPTION |
|---|---|---|---|
| LOW | 2250863 | XX-CSC-IN-MM | Missing authorization check in CIN Journal Voucher |
| LOW | 2748063 | BC-SEC-LGN-SML | Improper Session Management in ABAP Server of SAP NetWeaver and ABAP Platform |

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