LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

April 2019

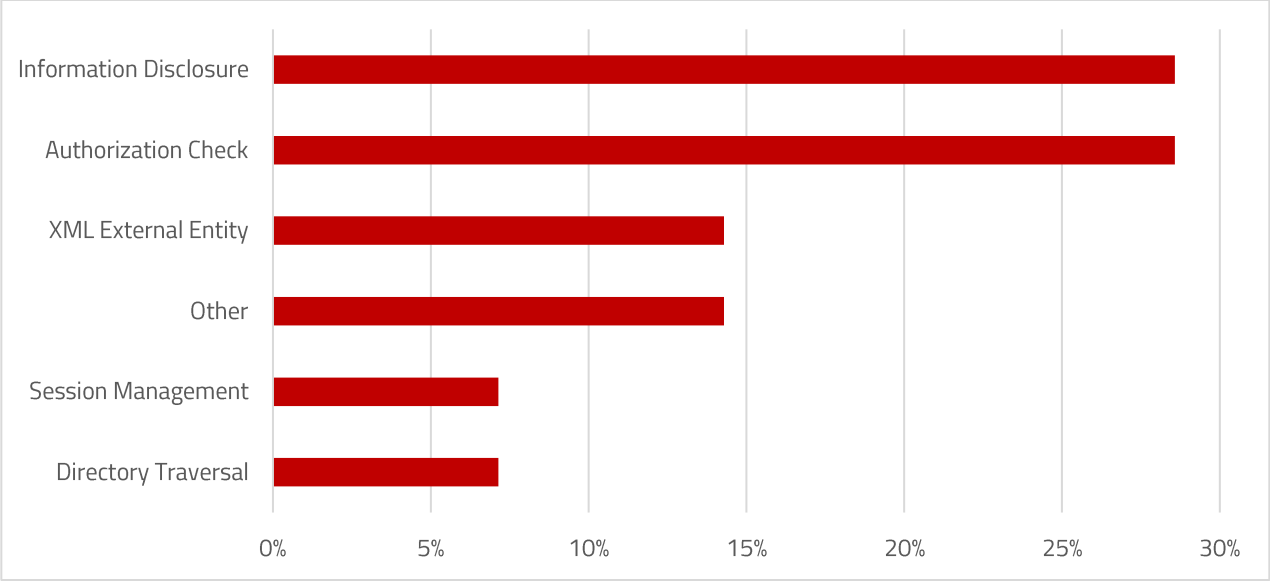
SAP Security Notes

April 2019

Note 2747683 patches a vulnerability in the signature security mechanism of the Adapter Engine in SAP NetWeaver Process Integration (PI). The vulnerability could enable attackers to spoof XML signatures and send arbitrary requests to the server via PI Axis adapter. Such requests will be accepted by the PI Axis adapter even if the payload has been altered, especially when the signed element is the body of the xml document. SAP has corrected the relevant code in PI Axis Adapter. The corrections apply additional checks for signed elements for correctness before signature validation. Customers should apply the relevant support packages and patches referenced by SAP Note 2747683.

Note 2776558 provides corrections for a high-risk insufficient authorization check in SAP Funding Management. The vulnerability could be exploited to escalate privileges and carries a CVSS score of 8.3/10.

Notes 2742758 and 2741201 deal with information disclosure vulnerabilities in in the messaging system and runtime workbench of SAP PI. This could lead to the leakage of sensitive system information that could be exploited to perform further attacks against the platform.



SAP Security Notes by Vulnerability Type

Note 2687663 patches a similar vulnerability in the .NET SDK WebForm Viewer of SAP Crystal Reports. Sensitive database information that could be disclosed by exploiting the vulnerability include user credentials.

Appendix: SAP Security Notes, April 2019

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for the browser control Google Chromium delivered with SAP Business Client
HIGH	2776558	FS-TXS	Fehlende BerechtigungsprÃ¼fung in SAP Funding Management
HIGH	2747683	BC-XI-CON-AXS	[CVE-2019-0283] SAP NetWeaver Process Integration (Adapter Engine) vulnerable to Digital Signature Spoofing
HIGH	2687663	BI-RA-CRV	[CVE-2019-0285] Information Disclosure in SAP Crystal Reports
MEDIUM	2662687	IS-B-BCA-MD	[CVE-2018-2484] Missing Authorization check in SAP Enterprise Financial Services
MEDIUM	962319	BC-WD-JAV-RUN	Detailed error messages with stack trace in Web Dynpro
MEDIUM	2729710	BC-CCM-SLD-REG	[CVE-2019-0265] XML External Entity (XXE) vulnerability in SLD Registration of SAP NetWeaver and ABAP Platform
MEDIUM	2643447	BC-ABA-LA	Directory Traversal vulnerability in ABAP Server File Interface
MEDIUM	2643371	BC-ABA-LA	Missing Authorization check in ABAP Server File Interface
MEDIUM	2753629	BC-INS-FWK	[CVE-2019-0279] Missing Authorization check for ABAP INST function module
MEDIUM	2748048	BC-SEC-LGN	Leverage of privileges in ABAP Server of SAP NetWeaver and ABAP Platform
MEDIUM	2772376	HAN-DB	[CVE-2019-0284] XML External Entity vulnerability in SAP HANA sldreg
MEDIUM	2742758	BC-XI-IS-WKB	[CVE-2019-0282] Information Disclosure in NetWeaver PI Runtime Workbench
MEDIUM	2741201	BC-XI-CON-MSG	[CVE-2019-0278] Information Disclosure in the SAP NetWeaver Process Integration (Messaging System)

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