LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

March 2018

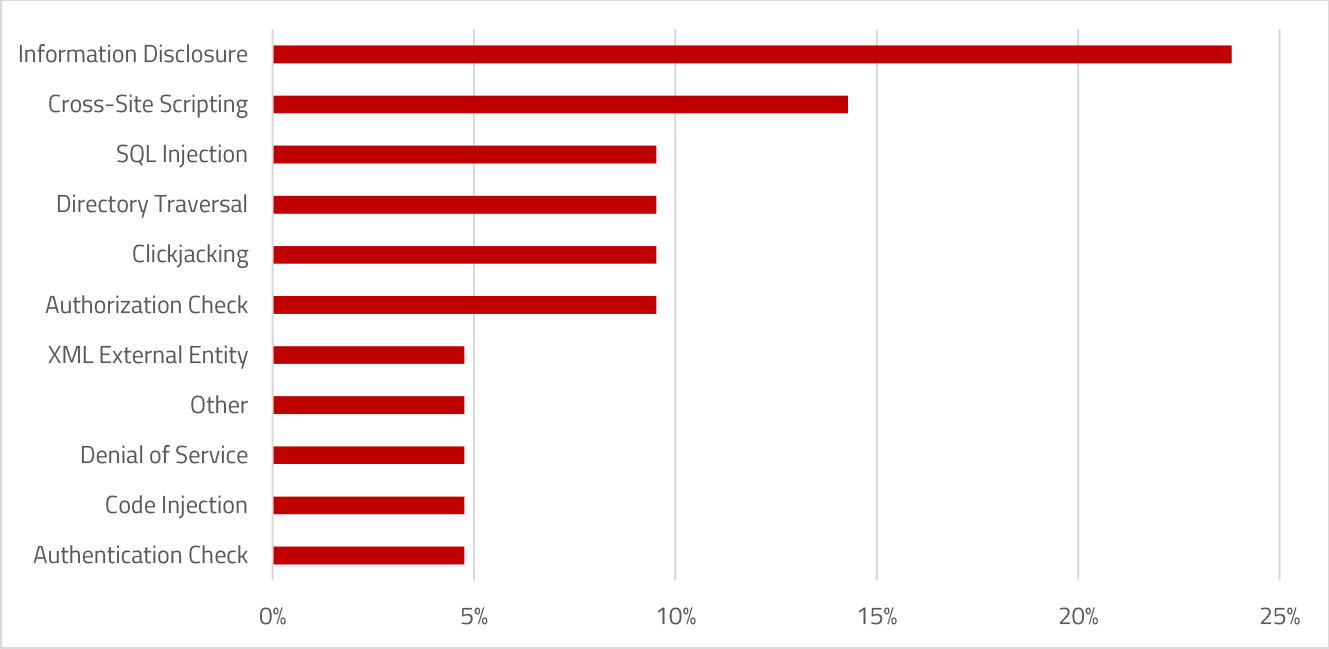
Note 2331141 addresses a high-risk SQL injection vulnerability in the FI Localization tables of S/4HANA. The corrections included in the support packages listed in the note will enable screening of user input for dangerous SQL statements. The formula expressions delivered in Note 2261750 are a prerequisite for user input validation checks delivered via the note.

Note 2604541 includes corrections in support packages for a dangerous denial of service and DDOS vulnerability in the Java OData Gateway. The vulnerability impacts vulnerable open-source Apache servlets that manage incoming OData requests. Refer to CVE-2017-12624 and CVE-2017-3156 for further details.

Notes 2596535 and 2587369 deal with information disclosure vulnerabilities in SAP Business Process Automation (BPA) by Redwood and SAP HANA 1.0 and 2.0. Both notes carry a CVSS score of 7.5 or higher and could be exploited to leak sensitive system and user-related data. In the case of SAP HANA, user credentials may be stored in clear text in indexserver trace files. Attackers may be able to access systems using compromised credentials garnered from the files. This requires TRACE_ADMIN or CATALOG READ privileges. Access to these and other critical privileges in HANA systems should be monitored using SAP Solution Manager.

SAP Security Notes

March 2018



SAP Security Notes by Vulnerability Type

Note 2595262 includes corrections for a cross-site scripting vulnerability in the SAP CRM WebClient UI. The note has multiple prerequisite notes including collective note 2577883.

Finally, Note 2538829 includes updated libraries for open-source components in the SAP Internet Graphics Server (IGS) that are vulnerable to remote code execution attacks that could lead to memory corruption and provoke a denial of service.

Appendix: SAP Security Notes, March 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2331141	XX-CSC-RU	SQL Injection vulnerability in FI-LOC-FI-RU
HIGH	2604541	OPU-GW-JAV	Denial of service (DOS) in GWJPO
HIGH	2596535	XX-PART-REDWOOD-BPA	[CVE-2018-2400] Information Disclosure in SAP BPA BY REDWOOD
HIGH	2595262	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
HIGH	2538829	BC-FES-IGS	Open Source Software Security Vulnerabilities in SAP Internet Graphics Server (IGS)
HIGH	2587369	HAN-CPT-CPT2-CNR	[CVE-2018-2402] Potential information disclosure in SAP HANA capture & replay trace file
MEDIUM	2495144	FI-CF-INF	Switchable Authorization checks for RFC in Central Finance
MEDIUM	2169722	EP-PIN-AI	Whitelist based Clickjacking Framing Protection in Enterprise Portal
MEDIUM	2201710	BC-SYB-PB	Fixing Logjam and Alternative chains certificate forgery vulnerabilities in multiple SAP products
MEDIUM	1906841	XX-CSC-RU-FI	Potential disclosure of persisted data in XX-CSC-RU
MEDIUM	2051336	SV-SMG-DVM	Potential disclosure of persisted data in SV-SMG-DVM
MEDIUM	2555667	XX-PART-REDWOOD-BPA	[CVE-2018-2366] Directory Traversal vulnerability in SAP Business Process Automation by Redwood
MEDIUM	2550538	BI-BIP-CMC	[CVE-2018-2397] Cross-Site Scripting (XSS) vulnerability in SAP BI Central Management Console
MEDIUM	2580967	BC-FES-BUS-DSK	[CVE-2018-2398] Information Disclosure in SAP Business Client
MEDIUM	2597543	BC-INS-TLS	Directory Traversal vulnerability in SAPCAR
MEDIUM	2596766	XX-PART-REDWOOD-CPS	[CVE-2018-2401] XML External Entity vulnerability in SAP BPA BY REDWOOD
MEDIUM	2592807	BC-SRV-PMI	[CVE-2018-2399] Cross-Site Scripting (XSS) vulnerability in Process Monitoring Infrastructure
MEDIUM	2509307	FS-RI	Hard-coded credentials in FS-RI
MEDIUM	2509215	FS-RI	SQL injection vulnerability in FS-RI
MEDIUM	2142551	BC-WD-ABA	Whitelist service for Clickjacking Framing Protection in AS ABAP
LOW	2591244	SV-SMG-CM	ChaRM users are able to access changes they are not involved in

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

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.