Security Validation Report

SAP Sales Cloud CNS

Date of Report
2022-09-15

Overall Rating: ★★★★☆

Minor process gaps and low severity vulnerabilities identified from active validation. DPP compliant (Excludes SEC-256). Hyperscalers configuration issues identified during secure operations review.

Activity done	Result	Comment
Secure Development	★★★★☆	• ACD is well documented. Customer and Security documentation provided • Threat modelling performed, some of the threats are mitigated and threats which are planned(critical and medium) for mitigation have exception approval • PSC:14 requirements are planned to fulfill out of which 6 are TopX requirement and 1 TopX requirement is in not fulfilled state, all of these have exception approval • SAST: Checkmarx, sonar and fortify scans performed and issues are audited. • OSS: Whitesource scan performed and few medium severity vulnerabilities are open and are within SLA • Secure Operations: Multiple issues related to Hyperscalers configuration have been identified.
Vulnerabilities	★★★★☆	• 2 low severity issues identified during active validation
Data Protection & Privacy	★★★★☆	• There is an aligned roadmap (exceptional approval) in place for deletion requirement therefore we have skipped analysis of the same in the current validation • Read Access Logging: Application delivers the business pa rtner attachments download and thumbnails as sensitive personal data. Whenever a user views it, the system creates a Read Access Log (RAL) entry. • Consent requirement is not applicable • Data disclosure and Change history features implemented to fulfil the SEC-255 and SEC-265 • SEC-364 and SEC-363 requirements planned for Q4 2022

#	Issue Description	Tracking (System/Link/Message No.)	Status	Severity/ CVSS Rating
10	Product Standard Security Compliance: 14 requirements are planned to fulfill out of which 6 are TopX requirement | 1 TopX requirement is in not fulfilled state with exception approval Recommendations: • Fulfill the requirements as planned.		Open	Minor
11	OSS : Whitesource scans are performed and few medium severity vulnerable libraries are observed (within SLA) Recommendations: • Update all the vulnerable libraries to latest libraries.		Open	Minor
12	Threat Modeling: 1 critical(planned), 8 high(4 mitigated, 4 planned), 13 mediums(6 mitigated, 7 planned) and 1 low(planned mitigation) risk has been identified Recommendations: • Mitigate all the risks as planned.		Open	Moderate
25	User Management: AWS access keys not rotated for within 90 days of creation | Few access keys idle and not used for more than 90 days Recommendations: • Follow the Hyperscaler hardening guidelines provided by the requirement SEC-370.	STC4CPERF2021-2666	Open	Minor
26	Authorization: AWS IAM Roles have administrator access permissions | AWS MFA not enabled for IAM users Recommendations: • IAM roles should not have administrator access permissions. • Enable MFA for IAM users. • Following the Hyperscalers hardening guidelines provided by SEC-370.	STC4CPERF2021-2292	Open	Moderate

#	Issue Description	Tracking (System/Link/Message No.)	Status	Severity/ CVSS Rating
27	Secure Default: AWS - EKS endpoint publicly enabled | RDS database instance is in a public subnet Recommendations: • Follow the Hyperscalers hardening guidelines provided by SEC-370.	STC4CPERF2021-1653	Open	Moderate
28	Secure Default: AWS - ELB access log disabled Recommendations: • Access Log should be enabled.	STC4CPERF2021-2292	Open	Minor
29	Secure Default: AWS Elastic Load Balancer with listener is not configured with TLS/SSL Recommendations: • Harden as per Hyperscalers compliance.	STC4CPERF2021-2292	Open	Minor
16	Inscure CORS configuration Recommendations: • Properly configure the CORS headers.		Open	3.1
17	Missing JWT invalidation after logout Recommendations: • Invalidate the JWT after log out.		Open	3.5
18	SDOL-006: SEC-364 Conduct data transfer impact assessments on a regular basis & SEC-363: Engage subprocessors in a compliant and transparent manner: Planned for Q4 2022 Recommendations: • Fulfil the requirement as per the plan.		Open	Minor

SAP Sales Cloud CNS

Security Validation Level: 2

Security Validation Activities

Review provided documentation

- Architecture | Customer Documentation | Security Guide | Threat Modelling | Secure Operations

Conference call with developers

Manual runtime test focus: Session Management | Authorization | Configuration review | File upload

Tools: BurpSuite

Check code scan findings(SAST): Scans are performed using fortify, checkmarx and sonarqube, all the issues are audited as per guidelines

OSS scans are performed with whitesource and few medium severity libraries observed(within SLA)

Secure Operations Review:

- SEC-301: No DR agreements as part of customers contracts. Restoration possible from Backups and Infra DRs available
- SEC-303: Program is part of C4C - Cloud Native Stack and Breach notification is fulfilled by CX C4C
- SEC-307: All AWS accounts are now MFA enabled which is recommended by MultiCloud team
- SEC-308: AWS Cloud Trail logs are sent to Splunk and monitored by SGS | Use cases are defined and controlled by MultiCloud team
- SEC-311: Regular AWS Cloud and MongoDB backups are maintained | Restoration steps and test results are provided
- SEC-340: C4C Cloud Native CAM profiles exist for various support activities
- SEC-370: Following Hyperscaler configuration issues identified
  - AWS access keys not used for more than 90 days
  - AWS IAM access keys should be rotated within 90 days of creation
  - AWS IAM Roles should not have administrator access permissions
  - AWS MFA not enabled for IAM users
  - AWS Elastic Load Balancer (Classic) with access log disabled
  - AWS Elastic Load Balancer with listener TLS/SSL is not configured
  - AWS EKS cluster endpoint access publicly enabled
  - AWS RDS database instance is in a public subnet

Test landscape

Customer-like landscape requested for validation: YES

Tests performed on Validation system

Test landscape issues: NONE

Security Validation Coverage

Process review, Active testing, DPP, Secure Operations

Star Rating Matrix

	Corporate Requirement Violation					
Activity done	☆☆☆☆☆ (0)	★☆☆☆☆ (1)	★★☆☆☆ (2)	★★★☆☆ (3)	★★★★☆ (4)	★★★★★ (5)
Secure Development	>= 3 open Severe / Significant OR >=7 open Moderate	2 open Severe / Significant OR 6 open Moderate	1 open Severe / Significant OR 5 open Moderate	No open Severe / Significant, 4 open Moderate	1 - 3 open Moderate	No Severe / Significant issues found during AND no open Moderate at end of Security Validation
Vulnerabilities	1 open Vulnerability with CVSS >= 9	1 open Vulnerability with CVSS >= 8	1 open Vulnerability with CVSS >= 7	>= 5 open Vulnerabilities with CVSS < 7	1 - 4 open Vulnerabilities with CVSS < 7	No open Vulnerabilities at end of Security Validation
Data Protection & Privacy	>= 3 open Severe / Significant	2 open Severe / Significant	1 open Severe / Significant OR >= 4 open Moderate	1 - 3 open Moderate	All Severe / Significant / Moderate findings closed, open Minor	No Severe / Significant issues during AND no open findings at end of DPP Validation

Security Validation Wiki for Process Description and Frequently Asked Questions:

https://wiki.wdf.sap.corp/wiki/display/SecVal/Project+Close+and+Security+Validation+Report
https://wiki.wdf.sap.corp/wiki/display/SecVal/After+Project+Close+-+Handling+Open+Issues+for+RDM