oraclecms
customer management solutions

VULNERABILITY TESTING POLICY

Version:	v 1.9
Date of version:	12/09/2024
Created by:	James Paul
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
23/04/2017	1.0	Casey Eldib	Basic document outline
24/04/2017	1.1	James Paul	Reviewed/modified
18/07/2017	1.2	James Paul	Updated
09/08/2018	1.3	Fiona Nicholls	Updated/reviewed
03/09/2019	1.4	Di Parker	Reviewed/updated
13/09/2020	1.5	Mark Needham	Reviewed
09/09/2021	1.6	Mark Needham	Reviewed/updated
09/09/2022	1.7	Mark Needham	Reviewed/updated
11/09/2023	1.8	Mark Needham	Reviewed/updated
12/09/2023	1.9	Mark Needham	Reviewed/updated

TABLE OF CONTENTS

1. PURPOSE

The purpose of this policy is to establish guidelines and procedures for conducting vulnerability testing on all software developed and maintained by OracleCMS for contact center operations. This policy aims to ensure the identification and mitigation of potential security vulnerabilities to safeguard sensitive data and maintain the integrity of our systems.

2. Scope

This policy applies to all software developed and maintained by OracleCMS for contact center operations, including but not limited to:

- Customer relationship management (CRM) systems
- Communication platforms
- Call routing and management software
- Reporting and analytics tools

3. Vulnerability Testing Procedures

3.1 Frequency of Testing

Vulnerability testing will be conducted regularly throughout the software development lifecycle, including during the design, development, testing, and deployment phases. Additionally, periodic scheduled vulnerability scans will be performed on production systems.

3.2 Types of Testing

a. **Static Analysis:** Source code analysis will be conducted using automated tools to identify potential vulnerabilities during the development phase.

b. **Dynamic Analysis:** Dynamic testing will be performed on running systems to identify vulnerabilities related to configuration, authentication, and input validation.

c. **Penetration Testing:** Periodic penetration tests will be conducted by qualified security professionals to simulate real-world attacks and identify vulnerabilities that may not be detected by automated tools

3.3 Responsibilities

- The development team is responsible for conducting static analysis and addressing any vulnerabilities identified during the development process.
- The security team is responsible for performing dynamic analysis and penetration testing, as well as coordinating with external security experts if necessary.
- Project managers are responsible for ensuring that vulnerability testing is integrated into the software development lifecycle and that vulnerabilities are addressed in a timely manner.

4. Vulnerability Prioritisation

4.1 Rick Assessment

Vulnerabilities will be prioritised based on their severity and potential impact on the confidentiality, integrity, and availability of systems and data. The Common Vulnerability Scoring System (CVSS) will be used to assess the severity of vulnerabilities.

4.2 Prioritisation Criteria

a. **Critical (CVSS Score 9.0 - 10.0):** Vulnerabilities that pose a severe risk to the security of systems or data, such as remote code execution or SQL injection.

b. **High (CVSS Score 7.0 - 8.9):** Vulnerabilities with significant potential impact, such as privilege escalation or authentication bypass.

c. **Medium (CVSS Score 4.0 - 6.9):** Vulnerabilities that could lead to exposure of sensitive information or compromise system integrity.

d. **Low (CVSS Score 0.1 - 3.9):** Vulnerabilities with minimal impact or limited exploitability, such as information disclosure or cross-site scripting (XSS).

4.3 Response Time

- Critical and high-severity vulnerabilities must be addressed immediately upon discovery, with patches or mitigations deployed as soon as possible.
- Medium-severity vulnerabilities should be addressed in a timely manner, with patches or mitigations implemented within a reasonable timeframe.
- Low-severity vulnerabilities may be addressed during regular maintenance cycles, but should not be neglected if they pose a potential risk to security.

5. Reporting and Documentation

5.1 Vulnerability Reports

- Comprehensive reports detailing all vulnerabilities discovered during testing will be generated and documented.
- Reports will include details such as vulnerability type, severity, affected components, and recommended remediation actions.

5.2 Incident Response

In the event of a confirmed security incident resulting from a vulnerability, incident response procedures will be followed as outlined in the company's incident response plan.

6. Compliance and Review

6.1 Compliance

This policy complies with relevant industry standards and regulations, including but not limited to ISO 27001 and PCI DSS.

6.2 Policy Review

This policy will be reviewed and updated annually or as necessary to reflect changes in technology, regulations, or business requirements.

7. Validity and Document Management

This document is valid as of 12th September 2024.

The owner of this document is CTO, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents related to unacceptable or unauthorised use of information assets
- Number of incidents related to inappropriate employee training or awareness programs regarding acceptable use of information assets

Chief Technical Officer