A MITEL
TECHNICAL
PAPER

MiSDLC - Mitel Secure Development Life Cycle

Mitel Product Security

Release Date: April 2025
Revision: 1.1

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks .

Table of Contents

Purpose

This paper provides an overview of the Mitel Secure Development Life Cycle (MiSDLC), Mitel’s commitment to MiSDLC, the customer benefits and the key aspects of MiSDLC. This paper also covers the key components of Mitel’s Product Security Incident Response Team.

Mitel Secure Development Life Cycle - MiSDLC

Mitel Secure Development Life Cycle, MiSDLC, is a comprehensive framework to address product security and data privacy throughout the product life cycle. MiSDLC includes effective governance, security practice standards and guidance, measurement, and continuous improvement.

As news headlines keep illustrating, the world is continuously changing and the frequency, severity, and sophistication of attacks against communications infrastructure and products have increased and will, unfortunately, continue to increase.

MiSDLC provides managers, developers, and testers with a framework for embedding security and privacy best practices into the entire product development process. With a focus on continuous improvement, MiSDLC ensures we deliver secure solutions today and continue to address evolving security challenges going forward.

MiSDLC is a product development security assurance process that is based on the Open Web Application Security Project, Software Assurance Maturity Model, or OWASP SAMM, and related industry best practice guidance. OWASP SAMM is an open framework that is designed to assist organizations with the creation of their own Secure Development Life Cycle process while focusing on addressing the organization's specific security and privacy risks. To ensure that the product development process is fast and flexible, Mitel employs the Agile, Waterfall and DevOps software development models, and has customized Mitel’s secure development framework so that it integrates with these software development models.

Mitel's Commitment to MiSDLC

Mitel's commitment to MiSDLC is company-wide and encompasses all products currently developed by Mitel. The process applies to all personnel responsible for defining product requirements, product development, product testing, and support of Mitel components and products.

MiSDLC has been integrated into Mitel's Product Development Process, and all current Mitel products must comply with the MiSDLC process.

The MiSDLC process is designed to accommodate continuous process improvement, which in turn will result in continuous product improvements related to product security and the data privacy of the product's users.

Customer Benefits Resulting from MiSDLC

The MiSDLC process ensures that Mitel's customers realize significant benefits from products that have been developed with a sharp focus on product security and data privacy. Mitel’s customers benefit in several ways when using products that were developed in accordance with the MiSDLC process. For instance, products have less field found security vulnerabilities, which reduces risks for the customer, MiSDLC also assists customers with meeting their own security and privacy compliance requirements, and those of the end users.

The benefits of MiSDLC also extend beyond the product development process into Mitel's sales, deployment, and support organizations. The MiSDLC framework accomplishes this by infusing the Mitel culture with a heightened awareness of product security and privacy considerations while empowering all stake holders with the ability to contribute to the continuous product improvement process.

Key Aspects of the MiSDLC Process

To understand the MiSDLC process it is necessary to discuss the key aspects of MiSDLC. The MiSDLC process may be broken down into four business functions, and each business function is comprised of three security practices.

- **Governance** is the business function that governs the MiSDLC process, and the personnel participating in the process; the following security practices are used to ensure effective governance:
    - **Strategy and Metrics:** Manages the overall strategic direction of the MiSDLC program and uses metrics to focus security efforts and accelerate MiSDLC improvements.
    - **Policy and Compliance:** Establishes and maintains security policies and standards within a compliance and audit framework.
    - **Education and Guidance:** Provides role-specific security training and guidance to product development personnel.
- **Design** is the business function that determines what the product security requirements are and how the product should be designed to meet these requirements; the following security practices are instrumental in ensuring that the design meets the requirements:
    - **Threat Assessment:** Characterizes security threats to a product so that appropriate security and privacy controls can be implemented.
    - **Security Requirements:** Ensures the explicit inclusion of security-related requirements during the development process to specify correct functionality from inception.
    - **Secure Architecture:** Bolsters the design process by promoting secure-by-default designs and recommending secure technologies and components.
- **Verification** is the business function that ensures that the product meets Mitel security requirements. The following security practices are instrumental in ensuring that the security requirements have been met:
    - **Design Review:** Ensures that the design is compliant with Mitel product security standards.
    - **Implementation Review:** Assesses source code to avoid potential vulnerabilities and establishes a baseline for secure coding expectations.
    - **Security Testing:** Tests the product both with source code scans and in its runtime environment to identify and remediate potential vulnerabilities, as well as ensure compliance with Mitel quality standards for software releases.
- **Operations** is the business function that ensures the product is correctly deployed and configured for the customer so that product security and the customer's data privacy are optimized. The operations business function also provides the process and infrastructure to manage any security issues or incidents after the product has been deployed. The following security practices are required to support the operations business function:
    - **Issue Management:** Establishes a consistent process for managing internal and external vulnerability reports, Mitel product security incidence response program (which is described below); metrics from the program are used to enhance the security assurance program.
    - **Environment Hardening:** Implements controls for the operating environment surrounding the product to bolster the product's security.
    - **Operations Enablement:** Identifies and documents security-relevant information needed by an operator to properly configure, deploy, and operate the product.

Mitel's Product Security Incident Response Team

As part of Mitel's ongoing commitment to customers and product excellence, Mitel maintains a dedicated product security incident response program. The product security incident response program is included within the MiSDLC process.

The Mitel Product Security Incident Response Team (PSIRT) provides direct support for potential vulnerabilities identified in Mitel products. Mitel PSIRT will investigate and disclose vulnerabilities for actively supported products as per the Mitel Product Security Vulnerability Policy.

Mitel will work with customers, partners, and recognized security organizations to resolve detected security vulnerabilities.

Security Incident Reporting Process for Mitel Authorized Partners

Mitel Authorized Partners are advised to raise an incident regarding security-related inquiries directly with their regional Mitel product support group according to existing support processes. This path is the most expedient process for partners while use of the technical support process also provides partners with access to service request updates as they happen. Current software assurance and valid product certifications will be required.

Security Incident Reporting Process for Mitel Customers

Mitel customers are advised to contact their maintainer / Authorized Partner with any product security-related inquiries. The Authorized Partner will ensure sufficient details are collected prior to raising the issue with the relevant Mitel product support groups. The support team has an established process to escalate to Mitel PSIRT.

Security Incident Reporting Process for Non-Mitel Customers

Non-Mitel Customers can submit reports of potential vulnerabilities in Mitel products via email psirt@mitel.com.

The use of PGP to encrypt sensitive information sent via email is recommended; the Mitel PSIRT PGP key is published on the Mitel Product Security Policy web page. Please note that the psirt@mitel.com email address is not for general inquiries or support requests. .

Security Policies and Publications

Mitel's Product Security Policy is available at: www.mitel.com/support/security-advisories/mitel-product-security-policy .

The Mitel Product Security Vulnerability Policy provides further information on the vulnerability management process for Mitel products and is available at: https://www.mitel.com/-/media/mitel/file/pdf/solutions/mitel-product-security-vulnerability-policy.pdf .

Mitel Product Security Advisories are available at: www.mitel.com/support/security-advisories

Information on General Data Protection Regulation (GDPR) and Your Privacy are available at: https://www.mitel.com/legal/gdpr .

Product specific documents related to Security and Data Protection for MiVoice products are available in the Mitel Document Center: https://www.mitel.com/document-center and for OpenScape products via https://www.mitel.com/login/unify-login .

Mitel's Data Processing Addendum (DPA) is available to enterprise customers whose personal data Mitel processes upon written request to gdpr@mitel.com.