Mitel Product Security Vulnerability Policy

Date: September 2024

Document: SDPOL-002

Version: 1.0

Notices

Trademarks

Contents

SDPOL-002
Product Security Vulnerability Policy
Version 1.0

Introduction

As part of Mitel's ongoing commitment to customers and product excellence, Mitel maintains a dedicated product security incident response program to handle the discovery of potential vulnerabilities and security flaws in products.

The Mitel Product Security Vulnerability Policy has been published to help Customers, Mitel Authorized Partners and Security Researchers understand how Mitel manages and discloses security vulnerabilities associated with Mitel's products and services.

Mitel encourages the reporting of potential vulnerabilities in our products and applications. This policy document is intended to provide Mitel customers, partners, and independent security researchers with clear guidelines on how to submit discovered security vulnerabilities to Mitel and provide information about how Mitel performs Vulnerability Disclosure.

Intended Audience

Mitel Employees, Mitel Authorized Partners, Customers and Security Researchers.

Applicability

The Mitel Product Security Vulnerability Policy applies to all currently supported Mitel Unified Communications products and product versions as defined in Mitel Support Service Coverage document and Mitel Product Lifecycle Policy, available in Mitel PowerUP accessible via https://miaccess.mitel.com . The policy applies to Mitel Unified Communications (UC) solutions and products deployed by Mitel partners and customers and Mitel operated cloud services. The scope does not include Mitel enterprise infrastructure such as mitel.com web site and partner portals which are covered by associated IT security vulnerability management policies.

Actively developed products are monitored for potential vulnerabilities throughout the development process, continuing when they are released for General Availability, until the End of Design Support. Products or Software revisions that have reached End of Life or End of Design Support are not actively monitored and in such circumstances Mitel customers are encouraged and advised to maintain their solution at a currently supported version.

Secure Product Development

Mitel is committed to ensuring the development of secure products that protect the operations and safeguard the information of our customers. This is achieved by utilizing the Mitel Secure Development Life Cycle (MiSDLC), a comprehensive security software development framework used to address product security and data privacy throughout a product's life cycle. MiSDLC is based on the Open Web Application Security Project, Software Assurance Maturity Model - or OWASP SAMM – and provides managers, developers, and testers with a structure for embedding security and privacy, with a focus on continuous improvement to address security and privacy, throughout a product's life cycle. Mitel's commitment to MiSDLC is company-wide and encompasses all new Mitel products or product versions being developed.

While all Mitel products must comply with the MiSDLC process, security vulnerabilities are a part of any software vendor's life and may still emerge after a product has been released. In this event Mitel's Product Security Incident Response Team (PSIRT) is engaged.

Security Vulnerability Testing and Monitoring

Mitel's own security testing includes the use of software composition analysis tools, penetration testing tools, web application security testing tools, and network vulnerability scanning tools. If a vulnerability is detected during internal security testing Mitel's PSIRT determines if the vulnerability may also impact existing already released products or versions and whether customers using them are at risk. Mitel PSIRT also manages vulnerabilities reported by external security researchers and customers who conduct their own security audits as described later in this document.

In addition to Mitel's own security testing, Mitel also monitors external sources for security vulnerabilities that may potentially affect Mitel products. These sources include:

- Vulnerability Information and Coordination Environment (VINCE),
- Media and social media sources
- Governmental organizations including vulnerability notification services e.g. Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities Catalog (KEV)
- Professional vulnerability information service providers, and
- Vulnerabilities that become known to the public through various external sources including via software vendor advisories.

Vulnerability information is consolidated from the different sources, analyzed, and delivered to the relevant product teams expediently by Mitel PSIRT.

Vulnerability Assessment

The Mitel Product Security Incident Response Team (PSIRT) is a global team that is responsible for responding to potential security vulnerabilities in Mitel products. Mitel PSIRT analyzes and confirms potential vulnerabilities, while supplying corrective measures to address validated issues, commensurate with the identified vulnerability. In addition, Mitel PSIRT, among other tasks, also defines and executes the processes and policies defined in this document.

Definition of "Product Security Vulnerability"

For the purposes of this policy a "Product Security Vulnerability" is defined as *a "flaw in a Mitel software or hardware product that could impair the product's designed and available capabilities regarding confidentiality, integrity, or availability."*

In most cases a confirmed security vulnerability will require a new software patch, update, or release, to be delivered by Mitel, to resolve the issue.

What is not Considered a "Product Security Vulnerability"?

Not every report of a security vulnerability that is received at Mitel is a valid report or applicable to a Mitel product. Some examples of the type of reports that are not considered as being valid security vulnerabilities for the purposes of this policy include:

- If a reported vulnerability can be resolved by performing hardening steps. An example might be the use of simple or shared passwords - instead of choosing an individual, complex one.

- The intentional use of a feature or (mis)configuration setting that is weaker than the current recommended security best-practice. In some scenarios a trade-off between security and other interests (such as ease of use, backwards compatibility, performance, operational costs) may be made.
- The designed or intentional lack of a product security capability. For example, if a product has implemented only one administrative role or level. The risk is that every user of the product may exceed their privileges by being able to modify data, although not authorized. This is not a vulnerability of the existing product. However, it may be reported by a customer or researcher and be considered as a future recommendation for a feature enhancement in a later version of the product.
- Similarly updates to security protocols or practices that are made available after the release of the product version will be considered for future security hardening improvements. For example, updating from TLS 1.2 to TLS 1.3 in product versions released prior to the widespread deployment of TLS 1.3 will be considered as a future enhancement.

Mitel reserves the right to deviate from these definitions if required.

Vulnerability Categorization

Security vulnerabilities are further categorized as belonging to one of the following three categories:

1) The vulnerability is part of software developed by Mitel and included in one or more Mitel products.
2) The vulnerability is caused by a third-party software component that is embedded in one or more Mitel products.
3) The vulnerability is caused by the environment, where Mitel products run such as the Operating System where an application has been installed, or products of other vendors to which the Mitel application(s) connect.

Mitel's Product Security Vulnerability Policy is applicable to vulnerabilities detected in software developed by Mitel.

Mitel's Product Security Vulnerability Policy is also applicable to third party software components that are embedded in Mitel software and that cannot be independently updated or patched by the customer. For example, a product with an embedded Operating System (OS). This is usually described in the individual product's documentation or release note. If in doubt, customers should consult with their service partner or Mitel account representative for clarification.

The Product Security Vulnerability Policy does not apply to environmental vulnerabilities. To consider environmental vulnerabilities in their vulnerability and patch management processes customers are advised to refer to the corresponding vendor's security advisories and software release cycles, as well as compatibility matrices that are relevant to the customer's individual solution setup.

Figure 1 marks the typical borders where a security vulnerability requires remediation provided by Mitel or by a third party vendor (red boxes).

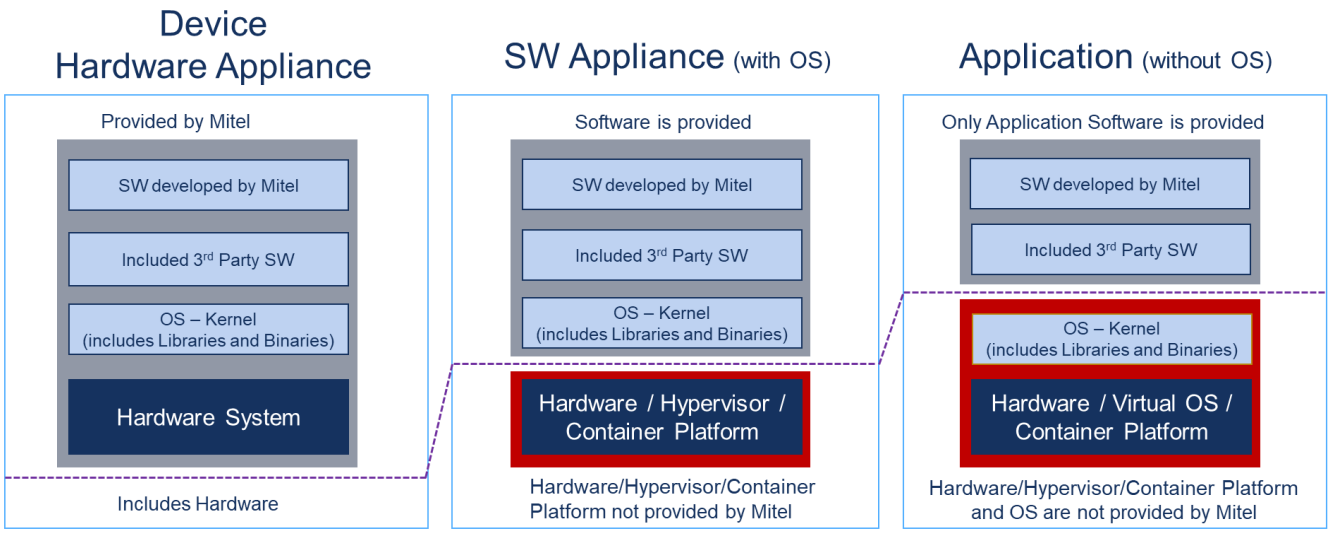

Figure 1 − Product Types and Example Vulnerability Disclosure Coverage

- **Device / Hardware Appliance** – Commonly this is a “closed” device/appliance where Mitel provides support for both the Operating System (OS) and applications to the customer and the customer does not typically have access to upload OS changes. In this case Mitel provides vulnerability support for the whole device/appliance.
- **Software Appliance** - Mitel is providing vulnerability support for the Mitel developed application and the underlying OS. However, Mitel is not providing Vulnerability Disclosure for the customer provided virtualization/container infrastructure or physical server. It is application specific as to whether the OS is included as a part of the software appliance or not. It is included if the OS cannot be independently updated by the service partner or customer. It should be noted that Mitel Standard Linux is covered by the policy.
- **Applications -** Mitel provides Vulnerability Disclosure for the Mitel developed application only. The customer is responsible for providing any infrastructure vulnerability resolutions.

Assessing a Security Vulnerability

Security vulnerabilities are assessed by the PSIRT for their relevance to Mitel products. There are generally four possible assessment outcomes for each potentially affected product:

- "**False Positive**": Although a vulnerability was initially reported against a product, further analysis has concluded that the product is not affected. This is a frequent outcome for reported vulnerabilities. It is quite common, for example, with embedded third party software component vulnerabilities that the concern only affects a portion of the software component, and that portion is not in use. Or it may be that the vulnerability is not exploitable in the context of the product. By default, Mitel PSIRT does not proactively inform customers about false positives.
- “**Configuration Solution**”: The reported vulnerability can be resolved without a software update in the affected product, but instead by making configuration changes to the systems or product’s environment,

as shown in the related product technical documentation. Mitel PSIRT decides on an individual vulnerability case basis whether customers need to be informed through a Security Advisory of these scenarios. In most cases it is only applicable if the proposed configuration settings are not already in the documentation or if a significant risk is seen for customer installations.

- "**Security Hardening Request**": While reported as a vulnerability, the raised concern is assessed as being not an exploitable vulnerability. In these cases, the concern will be considered for a future security improvement to the application/product.
- "**Confirmed Product Security Vulnerability**": The reported vulnerability is confirmed as a flaw by Mitel in the application or product and requires a resolution. Confirmed security vulnerabilities are prioritized according to the criteria described in the "Prioritization of Security Vulnerabilities" section.

Once a security vulnerability has been confirmed, Mitel will provide solutions commensurate of the exposure identified. The remediation provided remains at the sole discretion of Mitel

Prioritization of Security Vulnerabilities

The following factors contribute to determining the urgency and prioritization of a resolution for a vulnerability:

- Reported priority - the initial severity level / score given by the vendor of the affected software component or the reporter of the vulnerability.
- Mitel's evaluation of the vulnerability severity based on the impact on the product and its users. Mitel will assign a Mitel Severity level after the assessment.
- The effort required to exploit the vulnerability and whether there are already known exploits that impact Mitel's products.
- Whether there are effective countermeasures available that can mitigate the risk or not.
- And whether more than one Mitel product is affected? If so, there may be a different risk level and priority for each product.

Mitel uses the industry-recognized Common Vulnerability Scoring System (CVSS) as part of its process to evaluate the severity of potential vulnerabilities in Mitel products. (More information about CVSS is available at FIRST.org). The vulnerabilities are initially classified according to version 3.1 of the Common Vulnerability Scoring System (CVSS). CVSS 3.1 provides three measures, namely the Base, Temporal, and Environmental calculations. Mitel provides the CVSS 3.1 Base score and calculates a vulnerability severity vector and score ranging from 0 to 10. Mitel also provides a severity level to classify vulnerabilities in a simpler form.

The CVSS Base score is only one of the inputs used by Mitel to prioritize a vulnerability. In some cases, Mitel may use additional factors not adequately captured in the CVSS base metric to assess severity level. In these cases, these additional considerations will be described in the Security Advisory.

Customers are encouraged to consider the CVSS environmental metrics for their specific deployment which include factors such as mitigations within their environment to inform and prioritize responses for their deployments.

When exposure is confirmed in Mitel products and the following rating system is used:

Prioritization	Mitel Severity Level	CVSSv3.1 Score and Qualitative Severity Rating
1	Critical	9.0-10.0 (Critical)
2	High	7.0-8.9 (High)
3	Medium	4.0-6.9 (Medium)
4	Low	0.1-3.9 (Low)
5	Information only	0.0 (None)

Table 1 − Priorities and Severity Level of Vulnerabilities

For vulnerabilities reported in third party components that have a published Common Vulnerability and Exposures Identifier (CVE-ID) and CVSS qualitative severity rating published in the National Vulnerability Database (NVD), the Mitel assessment of severity based on exposure and impact for Mitel products may differ from the worst case assessment reported by NVD. Mitel priority for resolution will be based on Mitel assessed severity and impact to the individual products affected.

For vulnerabilities in Mitel developed products, Mitel assessment of severity is reported by NVD in most cases, and so aligns with the assessment provided in the Security Advisory.

Vulnerability Communications

Security Vulnerability Notification

A key deliverable of the Product Security Vulnerability Policy is to provide customers reasonable and useful vulnerability information. This is done through the publication of Security Advisories and where necessary associated/linked Technical Support Knowledge Articles.

Vulnerability Disclosure Policy

Mitel's first and foremost concern is our customers. Therefore, Mitel does not publish any details publicly that could potentially be used to compromise products until mitigation is available to reduce or eliminate risk. Critical information is circulated directly to channel partners, distributors or customers in a timely manner as required.

Mitel respects the security considerations of all customers and does not provide advanced details outside of established channels.

Security Vulnerability Advisory Overview

Security Advisories are issued by Mitel PSIRT as required and are published to the Mitel website at: https://www.mitel.com/support/security-advisories. Typically advisories are published on a Wednesday, but Mitel may deviate from this as required by the vulnerability exposure.

The main purpose of a Security Advisory is to provide information for customers to be able determine for themselves:

- if their Mitel assets are affected and need to be protected,
- to assess both the probability and impact of a threat and
- to decide on the appropriate countermeasures.

The information provided in Security Advisories strives to strike a balance of providing enough information for customers to be able to perform their own risk analysis, while not providing details that might enable a bad actor to use the information negatively.

A Mitel Security Advisory contains the following information:

- **Summary:** A description of the vulnerability that contains sufficient information for customers to decide on the countermeasures, but it does not contain information that is too detailed to prevent malicious attackers from creating and/or executing effective exploits.
- **Affected Products and Solutions:** A list of the Mitel products, including version information, that are impacted by the vulnerability identified. This allows a customer to determine whether their individual solution might be at risk or not.
  Occasionally more than one product or version may be affected by a single vulnerability, in those scenarios, the advisory may contain information about products or versions that are still under investigation.
  In certain circumstances, for example if a particular vulnerability or security incident attracts high attention in the public, the PSIRT may decide to release an advisory, even if no Mitel product is affected.
- **Vulnerability Severity:** A brief summary of the severity of the vulnerability, including a Common Vulnerability Scoring System (CVSS) rating, as assessed by Mitel. With third party components this assessment may or may not be the same as the associated CVSS score associated with the vulnerability in the National Vulnerability Database (NVD).
- **Mitigations / Workarounds:** If applicable, available mitigation or configuration measures are provided on how to resolve the vulnerability without having to apply the prescribed software updates. This may include a link to an associated Technical Support Knowledge Article as appropriate to the product.
- **Solution / Recommended Actions:** In most cases the PSIRT recommends applying the associated product update release or patch provided by Mitel. Resolution details are provided in the Security Advisory or Technical Support Knowledge Article as appropriate to the scenario. The measures may address affected products as well as the customer's environment.
- **References:** An optional list of publicly accessible external links (URLs) may be contained in the advisory. The additional information assists customers with assessing their risk and planning their countermeasures more accurately.
- **Revision History:** Contains a brief description of the changes made to a particular version and its publication date.

Email Notification of Security Advisories

Customers and Authorized Channel Partners may subscribe to be automatically notified when a Security Advisory is published by Mitel PSIRT. By subscribing to the Security Advisory distribution list an email will be received whenever a new Security Advisory is published to Mitel's web site. To request to be added to the distribution list complete the form available at the bottom of the page at: https://www.mitel.com/support/security-advisories.

Security Advisory Feedback

Feedback regarding ambiguous description or errors contained in Security Advisories is welcomed. Customers should contact their service partner or Mitel account representative for clarification, consolidation, and appropriate forwarding.

Reporting of Security Vulnerabilities by Mitel Partners and Customers

Mitel encourages partners and customers to report potential vulnerabilities in Mitel products. (Independent security researchers should reference "Reporting of Product Security Vulnerabilities by Security Researchers " later in this document).

Prior to performing security testing customers are recommended to ensure that the systems under evaluation are running currently supported versions of software so that detection of vulnerabilities that have been resolved previously are not detected and reported.

Reporting Process for Mitel Authorized Partners

Mitel Authorized Partners are advised to raise a technical support request with Mitel regarding any product security concerns through 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 to contact Technical Support.

Before engaging Technical Support:

- Mitel recommends for the benefit of the customer that the software version being tested is current. Planned testing for security vulnerabilities should ideally target the latest software versions provided so that detection of vulnerabilities that have previously been resolved are not detected and reported.
- Evaluate whether the reported issue is considered a "Product Security Vulnerability" according to the definitions provided elsewhere in this document.
- Use available Mitel product-related information – especially Security Guidelines, Security Checklists, Technical Support Knowledge Base articles and additional hardening information – to determine if the issue may be a "false positive" or can be solved through configuration of the product or environment.
- Attach related scanning results/assessment reports with a description of the vulnerability identified.
- If applicable provide a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Note configuration settings that impact (or may impact) the vulnerability and that are relevant to reproduce

the flaw.
- Where applicable provide proof of concept or exploit code.

Note: PSIRT does not answer questions regarding the retrieval and the installation of associated product patches or fix releases mentioned in Security Advisories. Please follow the standard maintenance and support processes.

Reporting Process for Customers

Mitel customers are advised to contact their service partner with any product security related inquiries or concerns as normal. The Mitel Authorized Partner will ensure that sufficient details are collected prior to raising the concern with the relevant Mitel product support groups.

Before engaging **planned** security testing services:

- Mitel recommends that, in coordination with the service partner, prior to any planned security testing that the software version being tested is current. Planned testing for security vulnerabilities should ideally target the latest software versions provided so that detection of vulnerabilities that have previously been resolved are not detected and reported.
- Evaluate whether any discovered concerns are considered a “Product Security Vulnerability” according to the definitions provided elsewhere in this document.

Use available Mitel product-related information – especially Security Guidelines, Security Checklists, and additional hardening information – to determine if the issue may be a “false positive” or can be solved through configuration of the product or environment.

As noted, customers should report product specific vulnerabilities via their service partner as normal. When reporting a potential vulnerability in a Mitel product via a service partner the following information should be included for the Partner to efficiently escalate the potential vulnerability:

- The name of the product that may have the vulnerability.
- The type of vulnerability (e.g., SQL injection, cross-site scripting, privilege escalation, buffer, or integer overflow etc.).
- Where applicable provide scanning results/assessment reports with a description of the vulnerability identified and the tools version used.
- Remove any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party) prior to sharing.

For Mitel customers without a current service partner, security vulnerabilities may be reported using the process below in “Reporting of Product Security Vulnerabilities by Security Researchers”.

How Mitel Partners and Customers Can Access Additional Information

Mitel MiVoice Portfolio: Mitel Authorized Channel Partners will have access to a product’s Release Notes through the Mitel MiAccess Web Portal available at https://miaccess.mitel.com via either the Knowledge Management System or Software Download Center.

Registered customers may also access Release Notes via the Mitel MiAccess Web Portal available at https://miaccess.mitel.com . If experiencing difficulty accessing the MiAccess portal, customers should contact

their service provider or Mitel account team.

Mitel OpenScape Portfolio:

OpenScape Partners may access Release Notes via the Partner Portal. Registered Customer may access the Release Notes via the Technical Support Web Support Portal available via https://www.mitel.com/support/mitel-technical-support .

Reporting of Security Vulnerabilities by Security Researchers

Mitel encourages independent security researchers or teams to report potential vulnerabilities in Mitel products. (Customer and Partners should reference "*Reporting of Security Vulnerabilities by Mitel Partners and Customers*" earlier in this document).

Authorization

If a security researcher makes a good faith effort to comply with this policy during their security research, Mitel will consider the research to be authorized and will work with the researcher to understand and resolve the issue quickly, and Mitel will not recommend or pursue legal action related to the research. Should legal action be initiated by a third party against a security researcher for activities that were conducted in accordance with this policy, Mitel will make this authorization known.

Guidelines

By participating in Mitel's vulnerability disclosure program Mitel expects that a security researcher:

- Has gained permission from the owner of any tested systems prior to performing any testing.
- Are not in violation of any applicable laws or breach of any agreements.
- Perform only the minimum non-destructive actions necessary to attain repeatable steps or proof of concept to confirm a vulnerability's presence.
    - Does not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Makes every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Notifies Mitel as soon as possible after discovering a real or potential security issue.
- Provides Mitel a reasonable amount of time to resolve the issue before public disclosure.
    - Mitel requests refraining from publicly disclosing any vulnerabilities until the issue has been addressed.

Once it is established that a vulnerability exists or any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party) is encountered, testing must stop and Mitel notified immediately, without disclosing this data to anyone else. Remove any sensitive data prior to sharing.

Authorization Scope

This Product Security Vulnerability Policy applies to Mitel Unified Communications (UC) systems and end devices (e.g. IP phones). The scope does not include Mitel operated cloud services, Mitel enterprise

infrastructure or internal web sites. Specifically, mitel.com and mitel.io web services are excluded from this authorization scope. Though Mitel develops and maintains other internet-accessible systems or services, Mitel asks that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that a security researcher believes merits testing, please contact Mitel to discuss it first.

Test Methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

Contacting Mitel

Security Researchers (and other non-Mitel customers) can submit reports of potential vulnerabilities in Mitel products via email to: psirt@mitel.com. When contacting the PSIRT communications must be in English.

Note: Please note that the psirt@mitel.com email address is not for general inquiries or support requests and general inquiries will not be responded to. For expediency customers should engage their service partner as normal for security support requests. Similarly, Mitel Authorized Partners should follow their established standard technical support process flow for security support. (also see "*Reporting of Security Vulnerabilities by Mitel Partners and Customers*" elsewhere in this document).

In case of confidential or sensitive information the use of PGP to encrypt the information sent via email is recommended and may be required for continued communications. The PSIRT PGP key is available at https://www.mitel.com/support/security-advisories/mitel-product-security-policy. In the event additional information / investigation should be required, Mitel PSIRT will respond directly to the reporter.

When reporting a potential vulnerability with a Mitel product include as many details as possible such as:

- The name and version of the product, including the installed fix/hot fix releases and patches, that the potential vulnerability is being reported against.
- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- The type of vulnerability (e.g.an SQL injection, cross-site scripting, privilege escalation, buffer, or integer overflow etc.).
- Attach related scanning results/assessment reports with a description of the vulnerability identified.
- Provide a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts, video or screenshots are helpful).
- Note configuration settings that impact (or may impact) the vulnerability and that are relevant to reproduce the flaw.
- Where applicable provide proof of concept or exploit code
- Any public disclosure plans.

What To Expect from Mitel

Upon receipt of the reported concern, the PSIRT team will send an acknowledgement email to the originator within 48 business hours and will start analyzing and validating the reported concern.

To the best of our ability, Mitel will confirm the existence of the vulnerability and be as transparent as possible about what steps are being taken during the remediation process, including on issues or challenges that may delay resolution.

If the investigation confirms a previously unidentified high risk vulnerability in Mitel products, Mitel will request a CVE number and publish a Security Advisory on the Mitel security portal when the resolution is generally available. If applicable, and desired by the reporter, at Mitel's sole discretion credit will be provided to the reporting researcher and their company within the associated Security Advisory.

Mitel will maintain an open dialogue to discuss issues and in cases where the vulnerability is confirmed, a disclosure timeline will be agreed upon. The agreement requires a per case decision that is dependent on the severity of the vulnerability and the potential risk in typical customer installations; as well as the required effort to address the vulnerability and provide a resolution.

Questions

Questions regarding this policy may be sent to psirt@mitel.com. Mitel also invites suggestions for improving this policy.

Annex A: Vulnerability Management for Mitel Cloud Services

The term Mitel Cloud Services relates to a set of services provided to customers and partners that are developed, implemented, and managed by Mitel.

With cloud services security and compliance is a shared responsibility between the data center vendor, the Mitel managed applications, the Mitel authorized channel partner (where applicable) and the end customer.

There are two main types of cloud services available from Mitel - Mitel Cloud Software as a Service (SaaS) and Mitel Hosted Unified Communications (UC).

Access to both cloud services is typically via a web browser or a Mitel provided client application that the customer has deployed to gain access to the cloud services.

General Provisions for Mitel Cloud Software as a Service (SaaS)

Mitel Cloud Software as a Services (SaaS) provide capabilities to the customer and/or service partner from the cloud. However access to these services is limited to configuration of the application(s) only for the service partner or customer. Examples of these types of services include Mitel CloudLink and Unify Phone. Typically these services are multi-tenanted.

With Cloud SaaS typically the hosting provider (e.g. Amazon or Google) is responsible for the hosting infrastructure including operating system, virtualization layer and in some cases the physical security of the data center. Mitel is responsible for the secure design, access, deployment, configuration, maintenance and operation of the SaaS applications. The service partner has limited access to the SaaS applications and is responsible for ensuring the secure deployment and configuration of the customer solution that uses the SaaS applications. The customer is responsible for ensuring the solution meets their security and compliance requirements.

The security measures defined within the MiSDLC process, and this Product Security Vulnerability Policy apply to the Mitel Cloud SaaS. However, the vulnerability disclosure procedures described earlier in this document only partially apply to Mitel Cloud SaaS as for these cloud services data center components and Mitel operated applications, it is Mitel that is responsible for the management and resolution of a security vulnerability. Therefore, as there is no action for the customer or partner to take, Mitel does not publish resolved vulnerabilities in Release Notes or publish Security Advisories for these cases.

For reporting of potential vulnerabilities, the previously described procedures should be followed.

General Provisions for Mitel Hosted Unified Communications (UC)

Hosted Unified Communications applications are Mitel applications that are deployed in a data center where the service partner (and customer) have implementation and configuration access to the both the application and, typically, its underlying operating system. Examples include Mitel’s MiCloud Flex and OpenScape Secure Cloud.

With hosted services, the hosting provider is typically responsible for the underlying hypervisor and host machines. The Operating System (OS) vendor is responsible for the security of the OS. Mitel is responsible for designing secure applications. The authorized channel partner is responsible for ensuring the solution is deployed securely as well as the day to day maintenance of the operating system and UC applications. The

service partner also ensures that any applicable operating system or application software updates are applied and configured. The customer is responsible for ensuring the solution meets their security and compliance requirements.

The security measures defined within the MiSDLC process, and the vulnerability disclosure procedures described earlier in this document apply to the Mitel Hosted UC applications.

For reporting of potential vulnerabilities, the previously described procedures should be followed.

Note: Some Mitel authorized service provider partners also provide hosted UC solutions using Mitel applications. In this scenario Mitel is responsible for the secure design of the application only. For this scenario the standard security vulnerability reporting and advisory processes are followed

Mitel Cloud Client Applications

Vulnerability Disclosure for Mitel client applications that provide access to Mitel Cloud Services is no different from the on-premises systems and applications processes described earlier in this document. Mitel Cloud client applications include:

- Mitel cloud Gateways and Probes used to provide cloud services.
- Mitel desktop clients accessing the cloud service.
- Mitel mobile clients for iOS and Android.
- Mitel browser extensions.

Customers, partners and independent security researchers may report security vulnerability concerns with cloud client applications as described earlier in this document. Mitel will disclose security vulnerabilities also as described earlier.

Annex B: Mitel Managed Services

Mitel offers various managed services in different geographic markets.

In some markets Mitel provides managed services to onsite deployed unified communications solutions through the local Mitel Direct Services team. In this scenario Mitel Direct Services is performing the service partner role that is referenced in this policy.

In a subset of these markets Mitel also provides managed Hosted Unified Communications (UC). There are two principal options available with Hosted UC. The first is where the Mitel Cloud Services team is acting in the service partner role and the other is where a service provider is performing this role - with Mitel Cloud Services providing the hosting services only.

If a customer is in doubt of their managed service the applicable contract should be referenced for clarification.

Document Change History

Version	Date	Description
1.0	09/27/2024	First release. Includes content from Mitel Product Security Policy and the Unify Vulnerability Intelligence Process (UFM-PLM-0009), which it supersedes.

References

[1]. Mitel Product Security Policy https://www.mitel.com/support/security-advisories/mitel-product-security-policy
[2]. Mitel Product Security Advisories https://www.mitel.com/support/security-advisories
[3]. CVSS (Common Vulnerability Scoring System) V3.1 https://www.first.org/cvss
[4]. Mitel Product Release Lifecycle Policy (DK120900) https://www.mitel.com/document-center/mitel-product-release-lifecycle-policy/all-releases/en/mitel-product-release-lifecycle-policy
[5]. Mitel Support Service Coverage (available in Mitel PowerUP via https://miaccess.mitel.com)