



Document Name: Coordinated Vulnerability Disclosure Policy

Policy Version: 1.0

Effective Date: 2026/09/09

Last Updated: 2026/09/09

Revision History:

Version	Date	Author	Description
1.0	2026/09/09	MiTAC Computing Technology Corporation, PSIRT Team	First release version

Preferred Reporting Channel: E-mail / Reporting Web Form

Policy Contact: psirt@mitacomputing.com

1. Purpose

MiTAC Computing Technology Corporation (“MiTAC Computing”) accepts and coordinates reports of potential vulnerabilities in its products and services.

This policy explains how to report potential vulnerability and what to expect during handling and coordinated disclosure.

2. Scope

This policy applies to supported products, services, software, firmware, hardware, components, online services, and environments managed by MiTAC Computing.

Information about supported products, versions, lifecycle status, and support conditions is available at: <https://www.mitacomputing.com/>

Anyone may submit a vulnerability report, subject to applicable law.

The following may be outside the scope of this policy:

- Products or services that are no longer supported;
- Systems, products, or services not owned, operated, maintained, or controlled by MiTAC Computing;
- Third-party systems not specifically listed as in scope;
- Test, development, demonstration, or discontinued environments listed as out of

scope;

- Activities or systems for which the reporter has no authorization.

Reports about unsupported or out-of-scope products may still be submitted. They will be assessed based on available information, risk, product status, and the organization's responsibility.

3. How to Report a Vulnerability

Report potential vulnerabilities through following official channel:

Text-Based or Web-Based Channels:

- E-mail: psirt@mitacomputing.com

The alternative channel may be used to:

- Request help with a vulnerability report;
- Provide initial information;
- Request information in an accessible format;
- Arrange a secure communication method.

For accessibility support or questions about this policy, contact:
psirt@mitacomputing.com

4. Secure Communication

Use an available secure method for sensitive vulnerability information, where appropriate.

Secure options may include:

- Encrypted e-mail using OpenPGP;
- Secure reporting form using HTTPS/TLS;
- Secure customer portal;
- Authenticated ticketing system; or
- Another approved secure channel.

5. Information to include in a vulnerability report

A vulnerability report should include, where available:

- The affected product, service, model, version, component, configuration, or environment;
- A summary of the potential vulnerability;
- Reproduction steps or proof-of-concept information;
- The potential cybersecurity impact.

Other helpful information may include:

- Expected and observed behavior;
- Logs, screenshots, traces, crash information, or other evidence;
- Affected functions, interfaces, data flows, privileges, or security controls;
- The environment or configuration where the issue occurred;
- Known affected users, systems, products, versions, or configurations;
- Related suppliers, components, libraries, services, or dependencies;
- Suggested remediation, mitigation, or workarounds;
- Any indication that the vulnerability is being actively exploited;
- Information concerning any known cybersecurity incident associated with the reported vulnerability;
- Previous reports of the same or a related issue;
- Previous, current, or planned public disclosure;
- Reporter contact details and preferred attribution, if provided.

Analysis report will not include unnecessary personal data, credentials, production data, confidential customer information, trade secrets, or other sensitive information unless needed to show the issue.

6. What to expect

We normally acknowledge reporter's vulnerability reports within 14 working days.

The acknowledgement may include:

- Confirmation of receipt;
- A report reference number;
- A request for more information;



- The expected next step.

MiTAC Computing may provide status updates during handling.

We may ask for more information to assess, reproduce, prioritize, coordinate, remediate, mitigate, or disclose the issue.

The timing and content of updates may depend on:

- The completeness of the report;
- The complexity and severity of the issue;
- Affected products, versions, users, or environments;
- Evidence of active exploitation;
- Available remediation or mitigation;
- Coordination with other affected parties;
- Legal, regulatory, contractual, or certification requirements;
- The reporter's availability and communication preferences.

An acknowledgement does not confirm that the issue is a vulnerability or set a remediation or disclosure date.

7. Confidentiality and coordinated disclosure

Non-public vulnerability information will be protected and shared only with persons who need it.

Information may be shared with relevant suppliers, maintainers, service providers, vendors, coordinators, CSIRTs, authorities, customers, or other parties when needed for assessment, remediation, coordination, or compliance.

MiTAC Computing does not normally require a blanket non-disclosure agreement before sending an analysis report. Specific confidentiality arrangements may be agreed for sensitive, complex, multi-party, or regulated cases.

The reporter and MiTAC Computing should coordinate public disclosure.

Disclosure timing may depend on:

- Remediation or mitigation availability;
- Risk to affected users;
- Evidence of active exploitation;
- Time needed to develop and verify remediation;
- Coordination with other affected parties;
- The risk of independent discovery or disclosure;
- Applicable legal, regulatory, contractual, or certification requirements;
- Other public-interest or cybersecurity concerns.

Information provided before full publication may include:

- Affected products or versions;
- Security update availability;
- Fixed versions;
- Installation or deployment instructions;
- Temporary mitigation or workarounds;
- Required user actions;
- The planned full-disclosure date.

Exploit details, proof-of-concept information, attack steps, sensitive technical details, or other information that could help exploitation may be withheld until full disclosure.

If the disclosure date changes, affected users will be told the new date without undue delay.

8. Security advisories and remediation information

Where applicable, MITAC Computing may publish:

- Security advisories;
- Security warnings or notifications;
- Security updates or patches;
- Remediation information;
- Temporary mitigations or workarounds;
- Configuration guidance;
- User instructions;
- CVE IDs or records;

- Other security information.

Security-related information may be published through:

- The MiTAC Computing security webpage;
- Product support webpage;
- Customer portal;
- E-mail notification;
- Security advisory distribution channel;
- Security update mechanism;
- Approved intermediary or coordinator;
- Another suitable channel.

Published information may include:

- A vulnerability description;
- Affected products and versions;
- Root-cause or weakness information;
- Severity or risk;
- Exploitation status and indicators of compromise;
- Available remediation;
- Temporary mitigation or workaround information;
- CVE IDs;
- Required user actions;
- Known limitations or residual risks;
- Reporter recognition, with the reporter's agreement.

Published information may be updated when material information changes.

9. Reporter Recognition

Where appropriate, MiTAC Computing may recognize or credit the reporter.

Before public credit is given, the reporter's preferred attribution and agreement will be confirmed.

Recognition may include but not limited:

- Credit in a security advisory;
- Credit on a security webpage;
- Inclusion in a researcher recognition list;
- A letter or certificate of appreciation;
- Participation in a reward or bug-bounty program;
- Another suitable method.

Recognition may be withheld for confidentiality, privacy, legal, contractual, sanctions, or security reasons.

10. Good-Faith Reporting

Good-faith vulnerability research and reporting are encouraged.

Research is generally considered to be in good faith when the reporter:

- Makes a reasonable effort to follow this policy;
- Acts to identify and report a potential vulnerability;
- Avoids unnecessary harm to products, systems, services, data, users, and others;
- Limits testing to what is needed to show the issue;
- Protects non-public and sensitive information;
- Promptly reports unintended access, exposure, or service impact;
- Makes a reasonable effort to coordinate before public disclosure.

Subject to applicable law and this policy, MITAC Computing will not start or recommend legal action against compliant good-faith researches.

11. Policy Updates

This policy may be updated when the following change but not limited:

- Reporting channels;
- Supported products and services;
- Product lifecycle or support arrangements;
- Organizational practices and capabilities;
- Legal, regulatory, contractual, or certification requirements;



- CVD arrangements;
- Relevant cybersecurity guidance and standards.

Material changes will be stated in the revision history.