

GASTEC PSIRT Vulnerability Disclosure Policy

September 11, 2026

GASTEC CORPORATION ("GASTEC," "we," "us," or "our") is committed to improving the security of the products and services we provide. This Policy describes the reporting channel, guidelines, and our response policy for individuals who identify vulnerabilities in our products or services.

1. Scope of This Policy

This Policy applies to reports of vulnerabilities in the products and services we provide to our customers.

2. Vulnerability Response Framework

We have established a Product Security Incident Response Team (PSIRT) to address security issues affecting our products and services. The PSIRT receives and assesses vulnerability reports, coordinates with relevant departments, and manages each case through completion.

3. Guidelines for Security Research and Testing

When conducting vulnerability research or testing, you must comply with all applicable laws, limit your activities to what is reasonably necessary to identify the vulnerability and report it to us, and avoid causing harm to GASTEC, users of our products or services, or any other third party. This Policy does not grant any new authorization to access or otherwise interact with our products, services, or systems beyond what is permitted by applicable law or by an agreement with GASTEC. In particular, you must not engage in any of the following activities:

- Accessing systems that GASTEC has not expressly authorized you to access, bypassing authentication, or engaging in any other form of unauthorized access
- Conducting denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, or any other activity that could interrupt a service or degrade its performance
- Disclosing to any third party personally identifiable information learned in the course of the research
- Infringing copyrights, privacy rights, or any other rights of a third party, performing operations beyond your authorization, or engaging in any other unlawful activity
- Viewing, obtaining, copying, modifying, or deleting personal information, trade secrets, or other confidential information beyond what is necessary to verify the vulnerability
- Altering, deleting, damaging, or corrupting GASTEC's or any third party's data beyond what is reasonably necessary to verify the vulnerability
- Introducing or executing malware or any other harmful program
- Engaging in phishing, social engineering, or any similar activity directed at GASTEC's officers, employees, users, or any other person
- Engaging in any other activity that violates applicable law or exceeds what is reasonably necessary to verify the vulnerability

4. How to Report a Vulnerability

Please send vulnerability information to the following email address:

security@gastec.co.jp

To help us review your report efficiently, please provide the following information to the extent possible:

- Your name, company or organization, department, and contact information
- An overview of the vulnerability and the circumstances in which it was discovered
- The name and version of the affected product or service
- Reproduction steps, sample code, and any other relevant technical information
- The expected impact and potential risks if the vulnerability is exploited

5. What Happens After You Submit a Report

As a general rule, we will acknowledge a vulnerability report within three business days of receipt. We will then review the report and, as necessary, coordinate with relevant departments to investigate and respond.

During the response process, we will keep the reporter informed of our progress to the extent reasonably possible. If we confirm a vulnerability, we will consider and implement appropriate measures, such as product updates or configuration changes, and may publish alerts or workarounds on our website as necessary. After completing our response, we will inform the reporter of the remediation and scope of impact to the extent reasonably possible.

6. Disclosure of Vulnerability Information

Our general policy is to follow coordinated vulnerability disclosure, under which information is disclosed after a fix or workaround has been prepared, with priority given to minimizing the impact on users.

We will determine the timing and content of any disclosure on a case-by-case basis, taking into account the severity of the vulnerability, the scope of affected users or products, and the potential impact on users. Where appropriate, we will coordinate the timing and content of disclosure with the reporter.

We ask reporters not to disclose or publish detailed information about a vulnerability to any third party until GASTEC has completed its investigation and response and the timing of disclosure has been coordinated with us.

7. Our Policy Regarding Reports Made in Accordance with This Policy

GASTEC will not pursue civil legal action against individuals who conduct vulnerability research and submit reports in accordance with this Policy solely on the basis of such research or reporting.

However, all research and testing must be conducted at the reporter's own risk. Activities that violate this Policy or exceed what is necessary to verify a vulnerability, and any reports based on such activities, are not covered by this provision.

8. Rewards and Recognition of Reporters

GASTEC does not operate a bug bounty program and therefore does not offer monetary or other rewards for vulnerability reports. We also do not identify reporters by name, organization, or otherwise in published advisories, reports, or similar materials.

We appreciate the cooperation of those who report vulnerabilities; however, please understand that we do not provide rewards or publicly acknowledge reporters by name or organization.

9. Revisions to This Policy

We may review and revise this Policy as necessary. The latest version will be published on our website.

By working collaboratively with those who report vulnerabilities, GASTEC will continue to improve the security of its products and services.