Green Packet Product Security Incident Response Team (PSIRT) Policy

Version 1.4

Jun. 2026

Introduction to GP PSIRT

Green Packet PSIRT (Product Security Incident Response Team) is the only channel within GP organization to manage vulnerability information; it receives, handles, and discloses security vulnerabilities related to GP's products and solutions. GP PSIRT follows industry standards such as ISO/IEC 30111 and ISO/IEC 29147 to handle the received security vulnerabilities.

GP PSIRT is also responsible for formulating GP's security incident management policy and security incident solution, analyzing vulnerabilities and patches released by system software providers and security organizations, and responding & handling security incidents released by customers, security organizations, and/ or any individuals.

Principles for vulnerability management

Building up and implementing a "global end-to-end network security assurance system" is always GP's priority development strategies. GP has established sustainable and trustworthy vulnerability management system in terms of policy, organization, process, and technology. The management system, in an open manner, works with external stakeholders to jointly address the challenge of vulnerabilities.

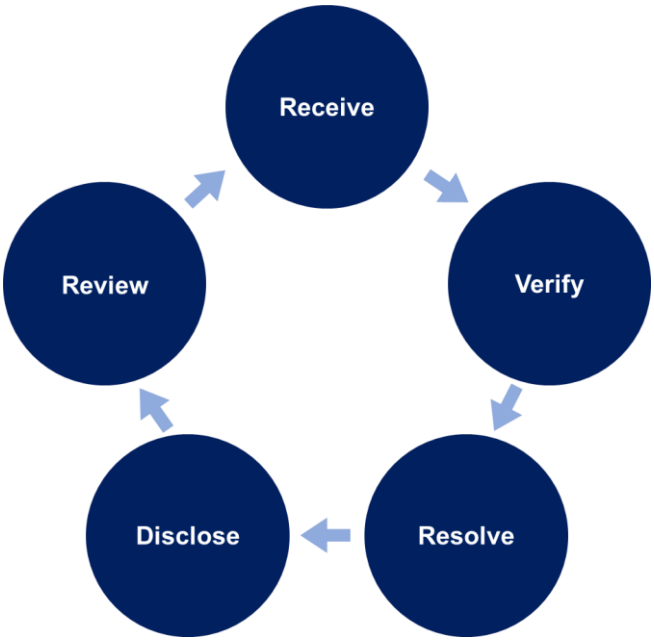
GP has proposed the following principles for vulnerability management:

1. **Collaboration in an open manner**: strengthen the collaboration and connection between the supply chain and the external security ecosystem, including the complete supply chains, security researchers & companies, security regulatory agencies, etc.
2. **Proactively reduce and mitigate vulnerabilities:**
   a). Take measures to reduce vulnerabilities in GP product and service;
   b). Once vulnerabilities in product and service are discovered, to provide customers/ users with risk reduction plans, corrective action plans and mitigation plans timely.
   c). Preventive action plans shall be in place consequently to ensure that similar vulnerabilities won't happen in the future again.
3. **Harm & damage reduction and risk control:** to reduce and eliminate the harm & damage caused to customers by vulnerabilities, and to reduce the potential security risks brought by vulnerabilities to customers/ users, is not just GP's vulnerability management principle and vision, but also the value guidance we follow in handling & disclosing vulnerability.
4. **Continuous improvement and optimization:** We continuously optimize the management workflow and specifications related to vulnerability management; and to implement the industry's standard and best practices to ensure our own management system stays optimized. During the process of vulnerability response, from "Receive, Verify, Resolve, Disclose, Review", GP PSIRT keeps communicating with the customer & related parties, synchronizing the latest progress with up-to-date time table & schedule plan, assisting the customer in

remediating vulnerabilities timely, and completing coordinated disclosure of vulnerabilities.

Vulnerability Response Process

GP conducts security governance that covers the complete supply chain, R&D, logistics, fulfilment, incident response, and various support fields, forming a cybersecurity assurance system throughout the whole product lifecycle. GP has established a complete vulnerability handling process in accordance with ISO/IEC and other standards to improve product security and ensure timely response when vulnerabilities are discovered.



1. **Receive:** To receive vulnerabilities that discovered from the various relevant party/ people (“P”). We encourage global security practitioners and industry organizations to send security vulnerabilities of GP products; we proactively search for threat intelligence released by the industry and identify effective vulnerability information as well. GP encourages various relevant party/ people (“P”) to report security vulnerabilities related to GP product and service.
   GP PSIRT Email:
   enquiries@greenpacket.ai

All the security vulnerabilities can be reported through the GP web portal www.greenpacket.ai

GP PSIRT will strive to respond to “P” within 24 hours by email upon receiving the report.

2. **Verify:** To verify vulnerabilities, analyze impacts, and assess risks.
   GP PSIRT analyzes and verifies security vulnerabilities; assesses & scores vulnerabilities in accordance with the industry standard.
3. **Resolve:** After confirming that a product/ service is affected by the vulnerability, to provide mitigation measures and solutions. For confirmed security vulnerabilities, GP PSIRT collaborates with our product team to formulate, develop, and provide vulnerability remediation solutions, effectively address security risks, and ensure the security & stability of customers’ data and system.
4. **Disclose:** To maintain communication, fix vulnerabilities and disclose vulnerabilities. During the process of vulnerability response, GP PSIRT keeps communicating with the customer & related parties, synchronizing the latest progress, assisting the customer in remediating vulnerabilities timely, and completing coordinated disclosure of vulnerabilities.
   Depending on the situation, GP PSIRT will disclose the resolution progress on a regular basis. Each safety issue report will be addressed within 3 months.
   Vulnerability List:

Description	Status	Planned completion time	Action
(example)			

5. **Review:** To accumulate experience from management, technology perspectives; to improve the efficiency and capability of vulnerability management. GP conducts managerial and technical root cause analysis, summarizes lessons learned, continuously optimizes vulnerability response processes, and improves product security to deliver secure products & services to customers.

Vulnerability Severity and Impact Rating

We assess the severity of suspected vulnerabilities in our products based on industry standards; we use Common Vulnerability Scoring System (CVSS) as part of its process of evaluating reported potential vulnerabilities in our products and services. The CVSS model uses three distinct measurements, or scores, that include Base, Temporal, and Environmental calculations; CVSS scoring provides a numerical means to quantify the severity of the vulnerability, and considers several factors, including the level of effort required to exploit a vulnerability as well as the potential impact should the vulnerability be exploited. We will summarize the assessed impact of a vulnerability by way of a qualitative representation of the severity, Severity Rating Scale (SRS), i.e., one of Critical, High, Medium, Informational.

Vulnerability Disclosure Policy

GP discloses and publishes the vulnerability information & remediation solutions in the following ways. GP provides the following types of security-related publications via the GP portal on www.gpdevice.com

Types of Security Publications:

1. SA (Security Advisory)

A security advisory includes the vulnerability **severity level**, **scope of affected products and versions**, **business impact**, and **remediation solution**. It is usually used to disclose the information and remediation solution of serious and high-risk security vulnerabilities of GP products; it provides detailed information about security issues that directly involve GP products and require an upgrade, fix, or other customer action.

2. SN (Security Notice)

A security notice includes a description of vulnerabilities that have impact on the industry, a description of relevant security topics, and GP's latest handling

progress for the vulnerabilities. SN provides information about security events that have the potential for widespread impact on customer networks, applications, and devices. It contains **summary information**, **threat analysis**, and **mitigation techniques** that feature GP products and services.

3. RN (Release Note)

A release note includes information about remediated vulnerability of GP product. RN is used to disclose issues with a Low Severity Rating Scale (SSR); RN is used to disclose security vulnerability that has been remediated in R&D processes such that customers can understand the product's security status.

External Communications

GP discloses and publishes the **SA** (Security Advisory) **& SN** (Security Notice) to support our customers to obtain the vulnerability information & remediation solutions in a timely and open manner. **RN** (Release Note) will be distributed to customers timely to ensure customers are staying informed of the latest product security status. Issues with a low severity rating are typically published as a bug Release Note (RN).

All the relevant exposures can be found on GP portal website.

Vulnerability Remediation

After investigating and validating a reported vulnerability, we strive to develop and qualify an appropriate remedy for products under active support from GP. A remedy can take one or more of the following forms:

- A new release of the affected product packaged by GP;
- A GP-provided patch that can be installed on top of the affected product;
- Instructions to download and install an update or patch from a third-party vendor that is required for mitigating the vulnerability;
- A corrective procedure or workaround published by GP that instructs users on

measures that can be taken to mitigate the vulnerability.

GP makes every effort to provide the remedy or corrective action in the shortest commercially reasonable time. Response timelines depend on many factors, such as:

Severity of the vulnerability;

Complexity of the vulnerability;

Scope of affectedness;

Effort/impact to remediate;

Product Life Cycle.

We will provide continuous security updates for GP's products and services.

The scope of vulnerability security updates includes latest security patches, vulnerability fixes, product hardware (firmware), pre-installed software, and/or external control software, third parties vendors' patch if required.

Usually, we will keep security updates for a certain device model until that product reaches the End of Sale (EoS) of its whole product life cycle, normally the product life cycle may last for at least 4-5 years depends on various factors. We may have security updates for certain models that last for longer until the Last Date of Support (LDoS), depending on the actual situation. The LDoS identifies the last date that GP will investigate and disclose product vulnerabilities.

Additional Information

1. GP PSIRT will strictly control the scope of vulnerability information, and to ensure it is only shared among those who directly involved in the vulnerability remediation process.
2. GP PSIRT has the right of interpretation for the above policy and strategy.