I. Overview

The Panasonic Product Security Incident Response Team (Panasonic PSIRT) will coordinate vulnerabilities reported to affect Panasonic products in accordance with the "Panasonic Vulnerability Coordination Policy".

The purpose of vulnerability coordination and disclosure by the Panasonic Group is to enhance the security of our products and to inform users of risks imposed by vulnerabilities in our products and how to reduce these risks.

The Panasonic Group business division producing the product affected by the reported vulnerability will release a mitigation in accordance with the "Panasonic Vulnerability Disclosure Policy".

This document contains Panasonic Group's vulnerability coordination and disclosure policies. The Panasonic Group reserves the right to modify the policies at any time.

II. Coordination Policy

A) How to contact Panasonic PSIRT with a vulnerability report

Vulnerability reports can be sent directly to:

-product-security@gg.jp.panasonic.com

or can be submitted through our reporting form:

-https://www.panasonic.com/global/corporate/product-security/sec/psirt.html

For reports via email, we recommend using PGP. Our PGP key can be obtained from the following URL.

Panasonic PSIRT PGP Public Key

https://www.first.org/members/teams/panasonic_psirt

After receiving a vulnerability report through either of the above methods, Panasonic PSIRT will send an initial response (acknowledgement) to the reporter within 3 business days. Periodic communication, including updates, will be maintained with the reporter as appropriate.

B) Definition of a Vulnerability

For this policy, a vulnerability is defined aa a weakness in the computational logic (e.g., code)

found in software, hardware, firmware or other products, where there is at least one exploitable scenario that negatively impacts confidentiality, integrity or availability.

C) Information that should be contained in the vulnerability report

1. The exact software version or model version affected (including a link to the product page)
2. A simple description of how the vulnerability was discovered (including what tools were used)
3. Proof of concept (PoC) code or instructions that demonstrate how the vulnerability can be exploited
4. Description of the impact of the vulnerability or a threat model that describes an attack scenario

When submitting a report, be sure to include any time constraints (for example, provide a date of publication or presentation at a conference if you know) that may apply.

After analyzing the report, Panasonic PSIRT will have a discussion with the business division in the Panasonic Group that developed the product with the reported vulnerability. After this discussion, Panasonic PSIRT will communicate to the reporter whether or not the reported issue is a vulnerability in accordance with the definition set in this policy.

D) What will Panasonic PSIRT do if the reported vulnerability affects a third-party library / component?

During the analysis of a reported vulnerability, if it is discovered that the vulnerability affects a library or component developed by a (non-Panasonic Group) third-party, Panasonic PSIRT and the business division using this third-party library or component collaborate to contact the developer of the affected library or component for remediation.

If necessary, Panasonic PSIRT may ask for assistance in coordinating a vulnerability with a third-party. Prior to doing so, Panasonic PSIRT will inform the reporter.

III. Disclosure Policy

Panasonic PSIRT will coordinate a disclosure with the affected business division for reported vulnerabilities. Once a remediation has been prepared by the business division, it will be disclosed. In any disclosure, the Panasonic Group will not include attack code or any unnecessary details that may cause attackers to gain an unfair advantage over defenders.

Upon request from the reporter of the vulnerability, Panasonic PSIRT will assign a CVE identifier for the vulnerability to be disclosed as a CVE Numbering Authority (CNA). The assigned CVE identifier will be provided to the reporter of the vulnerability.