Vulnerability Coordination and Disclosure Policy

Overview

The Haverford Systems, Inc. Product Security Incident Response Team (the “Haverford PSIRT”) will coordinate vulnerabilities reported to affected Haverford Systems, Inc. products, including products under the brands PTZOptics and HuddleCamHD, in accordance with the Haverford Systems, Inc. Vulnerability Coordination and Disclosure Policy, (the “Policy”).

The purpose of vulnerability coordination and disclosure by Haverford Systems, Inc. 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 Haverford Systems, Inc. division producing the product affected by the reported vulnerability will release a mitigation in accordance with the Policy.

This document contains Haverford Systems, Inc.’s vulnerability coordination and disclosure policies.

Why Haverford Systems, Inc. reserves the right to modify the Policy at any time.

Coordination Policy

How to contact Haverford PSIRT with a vulnerability report

Vulnerability reports can be sent directly to:
psirt@havsys.com
or can be submitted through our reporting form.
For reports via email, we recommend using PGP. Our PGP key can be obtained from the following URL: https://psirt.havsys.com/haverford-psirt-public-key.asc

After receiving a vulnerability report through either of the above methods, Haverford PSIRT will send an initial response (acknowledgment) to the reporter within 3 business days. For any reports sent in good faith, Haverford PSIRT will not pursue legal action against the reporter.

Definition of a Vulnerability

This Policy defines a vulnerability as an instance of one or more weaknesses found in software, hardware, firmware, configurations, or other products that can be exploited, causing a negative impact to confidentiality, integrity, or availability, or that allows the violation of an explicit or implicit security policy.

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, Haverford PSIRT will have a discussion with the Haverford Systems, Inc. division producing the affected product with the reported vulnerability. After this discussion, Haverford PSIRT will communicate to the reporter whether the reported issue is a vulnerability in accordance with the definition set in this policy.

Reported vulnerabilities and the status of coordination will be appropriately managed by Haverford PSIRT and the Haverford Systems, Inc. division producing the affected product.

During the coordination process, Haverford PSIRT or the Haverford Systems, Inc. division producing the affected product may inquire about the reported vulnerability. Any inquiries from the reporter will be promptly handled by Haverford PSIRT and the Haverford Systems, Inc. division producing the affected product. Working with the Haverford Systems, Inc. division, Haverford PSIRT will provide timely updates to the reporter on the coordination status of the reported vulnerability.

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

If, during Haverford PSIRT's analysis of a reported vulnerability, it is discovered that the vulnerability affects a library or component developed by a (non-Haverford System, Inc.) third-party, Haverford PSIRT and the Haverford Systems, Inc. division using this third-party library or component will contact the developer of the affected library or component for remediation.

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

Disclosure Policy

Haverford PSIRT will coordinate a disclosure with the Haverford Systems, Inc. division producing the affected product. Once the Haverford Systems, Inc. division producing the affected product prepares a remediation, Haverford PSIRT will coordinate public disclosure of the vulnerability. The vulnerability will be disclosed with a CVE identifier and a published CVE Record, along with a public security advisory or other appropriate remediation information.

In any disclosure, Haverford Systems, Inc. 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, Haverford PSIRT will work with MITRE Corporation or another CVE Numbering Authority (CNA) to obtain a CVE identifier for a vulnerability to be disclosed. The assigned CVE identifier will be provided to the reporter of the vulnerability.

Update History

2026/06/03	Initial Release