

HELIOS TECHNOLOGIES · PRODUCT SECURITY

Coordinated Vulnerability Disclosure Policy

How to report a potential security vulnerability in a Helios Technologies commercial product, and how the Helios Product Security Incident Response Team (Helios PSIRT) receives and evaluates reports.

SUBMIT REPORTS TO

psirt@heliostechnologies.com

APPLIES TO

Helios commercial products

Purpose

Helios Technologies, Inc. and its operating companies (together, “Helios”) recognize the value of the security research community and of customers and partners who report potential security issues. This policy explains how to submit a report about a potential vulnerability in a Helios commercial product, what Helios asks of people who submit reports, and the terms on which Helios accepts them.

The Helios PSIRT is the single point of contact for product security reports. Its practices are informed by recognized industry guidance for vulnerability disclosure and handling, including ISO/IEC 29147, ISO/IEC 30111 and the ISA/IEC 62443 series.

Scope

IN SCOPE

- Commercial hardware products sold by Helios and its operating companies, including hydraulic, electronic control and display products
- Firmware and embedded software in those products
- Configuration, programming and diagnostic software and mobile applications that Helios supplies for use with those products

OUT OF SCOPE

- Helios corporate websites, email and internal IT systems
- Third-party products, components or services, which should be reported to their vendor
- Denial-of-service testing, social engineering, phishing and physical attacks on Helios facilities or people
- Product support, orders, warranty and general quality questions, which should go to the relevant Helios operating company

How to submit a report

Send your report by email to psirt@heliostechnologies.com. Please write in English and send one report per potential vulnerability.

Email the Helios PSIRT

Opens a new email to psirt@heliostechnologies.com

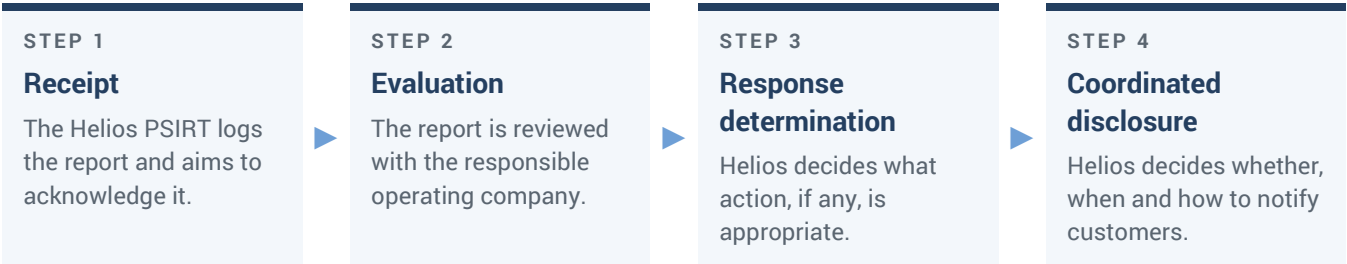
What to include

Information	Details that help the Helios PSIRT evaluate the report
Your contact details	Name, organization (if any), email address and preferred method of follow-up.
Product	Product name, operating company or brand, model or part number, and the firmware, software or hardware version(s) involved.
Description	The type of potential weakness (a CWE identifier, if known), the component or interface involved, and the conditions you believe are needed for it to occur.
Steps to reproduce	Step-by-step instructions, the test configuration, and any supporting material such as logs, screenshots or proof-of-concept code.
Potential impact	Your assessment of potential impact and, if you have calculated one, a CVSS score.
Disclosure status	Whether you have shared the information with anyone else (for example a CERT or coordinator), and any planned publication or presentation dates.

Sensitive information. Do not include personal data, credentials or customer information in your report. If you need to share sensitive technical details or large files, say so in your first email to psirt@heliostechnologies.com and the Helios PSIRT may arrange an encrypted method of exchange.

Immediate safety concerns. If you believe a situation presents an immediate risk to people, property or the environment, contact local emergency services and the operator of the equipment first. This reporting channel is not monitored around the clock.

How Helios handles reports



Receipt

The Helios PSIRT aims to acknowledge receipt of reports within a commercially reasonable time. Helios may contact you to ask for more information.

Evaluation

The Helios PSIRT reviews the report with the responsible Helios operating company to determine whether the information can be reproduced, which products and versions may be involved, and the relative severity of the reported issue. Helios may ask for your help in reproducing the reported behavior.

Response determination

If Helios determines that action is appropriate, it may develop and validate an update, mitigation, configuration guidance or other response. The nature and timing of any response depend on many factors, including the product, how it is deployed and the potential impact on customers' operations and safety. Helios may share general status information with you, at its discretion.

Coordinated disclosure

Subject to applicable law, Helios decides whether, when and how to publish a security advisory or notify customers. Where appropriate, Helios may coordinate with CERTs, CVE Numbering Authorities, regulators, suppliers and affected customers. Helios may be required by law to notify authorities about certain vulnerabilities, including those being actively exploited, and may do so before its evaluation is complete or before consulting you. Helios may consult you on the timing of disclosure. Helios asks you not to disclose any information about a reported issue publicly until Helios has had a reasonable opportunity to evaluate it and, where appropriate, make a response available to customers. If you intend to publish or present information about a reported issue, please tell the Helios PSIRT in advance and share a draft.

Guidelines for researchers

Helios products are often installed in industrial machinery and mobile equipment, where unexpected behavior can cause physical harm. When researching Helios products, please:

- Test only products and systems that you own or are explicitly authorized in writing to test.
- Never test equipment that is in operation, connected to machinery in use, or deployed in a customer environment.
- Stop testing immediately and report to Helios if your activity could affect the safety of people, equipment or the environment.
- Avoid accessing, modifying, deleting or keeping data that does not belong to you. If you encounter such data, stop, do not keep it, and tell Helios in your report.
- Do not degrade or interrupt the availability of any product, system or service.
- Keep information about the reported issue confidential until disclosure has been coordinated with Helios.
- Comply with all applicable laws, including export control and sanctions laws.

Terms of submission

By submitting a report to Helios, you agree to the following terms:

- **Voluntary submission, no compensation.** Your report is provided voluntarily. Helios does not operate a bug bounty program. Submitting a report does not entitle you to any payment, reward, public credit or other consideration, and creates no employment, agency or contractual relationship.
- **License to use.** You grant Helios and its affiliates a worldwide, perpetual, irrevocable, royalty-free, fully paid license to use, reproduce, modify, disclose and otherwise use the information you submit for any purpose, including evaluating, responding to and preventing security issues. This license does not extend to personal data, which Helios handles as described under Personal data below. You agree not to assert any claim against Helios arising from that use.
- **No confidentiality obligation on Helios.** Helios may share the information you submit with its affiliates, suppliers, CERTs, CVE Numbering Authorities, regulators, law enforcement and affected customers as Helios considers appropriate. Helios will not share your name or contact details outside Helios and its affiliates without your consent, except where required by law or where reasonably necessary to coordinate with a CERT or CVE Numbering Authority.
- **Your representations.** You confirm that you obtained the information lawfully and in line with this policy, that submitting it does not breach any law or agreement, that you have the right to submit it, and that you are not a person with whom Helios is prohibited from dealing under applicable sanctions laws.
- **No obligation to act.** Except as required by applicable law, Helios is not obligated to respond to, investigate, remediate or publicly disclose any report, or to follow any particular timeline. Any targets described in this policy are non-binding.
- **No admission.** Receiving or acknowledging a report, communicating with the reporter, evaluating a report, or taking any action in response is not an acknowledgement by Helios that a vulnerability or defect exists, or an admission of fault or liability of any kind.
- **Existing agreements unaffected.** This policy does not change any warranty, contract, terms of sale or other agreement between Helios and any customer, distributor or other party.

Personal data

Helios uses the personal data you provide, such as your name and contact details, to process your report and to communicate with you about it, as well as to meet Helios' legal and regulatory obligations. Because Helios is based in the United States, your data may be transferred to and processed in the United States and other countries where Helios operates, with appropriate safeguards where the law requires them. Helios handles personal data in line with applicable data protection laws, including the EU General Data Protection Regulation where it applies, and with the Helios privacy notice published at heliotechnologies.com. To ask about your personal data in connection with a report, contact psirt@heliotechnologies.com.

Legal notice. This policy is provided "as is," without warranty of any kind. Except for the Terms of submission and the commitments in the Guidelines for researchers section, it is not a contract and does not create any rights in favor of any person. It is not a representation about the security of any Helios product, system or service. Helios may change or withdraw this policy at any time, at its sole discretion and without notice. Changes do not apply to reports submitted before the change. The version published on the Helios website is the current version.

Questions about this policy may be sent to psirt@heliotechnologies.com.

Helios Technologies and the Helios logo are trademarks of Helios Technologies, Inc. Trademarks not belonging to Helios Technologies are the property of their respective companies.

Helios Technologies, Inc. · 7456 16th Street East, Sarasota, Florida 34243 USA

Publication HLIO-PSIRT-CVD-001-EN — October 2026 · Copyright © 2026 Helios Technologies, Inc. All rights reserved.