Hope Industrial Systems, Inc.

Toll Free (US): (877) 762-9790 • **International:** +1 (678) 762-9790 • **Fax:** +1 (678) 762-9789
1325 Northmeadow Parkway • Roswell, GA 30076 • USA • www.HopeIndustrial.com

Coordinated Vulnerability Disclosure Policy

Effective Date: September 11, 2026
Last Updated: September 11, 2026

Purpose and Scope

Hope Industrial Systems, Inc. ("HIS") is committed to maintaining the cybersecurity of its products and protecting its customers from cybersecurity risks. This Coordinated Vulnerability Disclosure ("CVD") Policy provides a process for customers, cybersecurity researchers, suppliers, and other parties to report suspected cybersecurity vulnerabilities affecting HIS products and supports HIS's obligations under Regulation (EU) 2024/2847, the EU Cyber Resilience Act ("CRA"), where applicable.

Reports may concern HIS products with digital elements, associated firmware or software, digital interfaces, product cybersecurity configurations or update mechanisms, and third-party components incorporated into HIS products. Product quality, warranty, repair, and general technical-support issues should be submitted through normal HIS customer-support channels.

Report a Vulnerability

If you believe you have discovered a cybersecurity vulnerability affecting an HIS product, please report it as soon as reasonably possible to the HIS Product Security Incident Response Team (PSIRT).

Product Security / Vulnerability Reporting

Email: psirt@hopeindustrial.com
Telephone: +1 (678) 762-9790
Website: https://www.hopeindustrial.com/support/cyber-resilience-act

To help HIS evaluate the report, please provide as much of the following information as reasonably available:

- HIS product model or part number and, if relevant, the serial number;
- firmware, software, or hardware version;
- a clear description of the suspected vulnerability and steps to reproduce or demonstrate the issue;
- the configuration or operating environment in which the issue was identified;
- the potential cybersecurity impact and any supporting logs, screenshots, or proof-of-concept information;
- whether you believe the vulnerability is currently being exploited or has already been publicly disclosed; and
- your preferred contact information.

Please avoid including confidential customer information, personal data, authentication credentials, or other sensitive information unless it is necessary to demonstrate or investigate the vulnerability.

Responsible Disclosure Guidelines

HIS supports coordinated vulnerability disclosure. When investigating or reporting a potential vulnerability, please:

- test only products or systems that you own or are authorized to test;
- do not exploit a vulnerability beyond what is reasonably necessary to confirm or demonstrate the issue;
- do not access, modify, destroy, retain, or disclose data belonging to another party, and avoid testing that could disrupt operations or system availability;
- respect privacy, third-party rights, and applicable laws; and
- provide HIS a reasonable opportunity to investigate and address the issue before publicly disclosing technical details that could facilitate exploitation.

HIS Response

After receiving a vulnerability report, HIS will make reasonable efforts to:

- acknowledge receipt when contact information has been provided;
- review, triage, and validate the reported vulnerability;
- assess the potential impact, severity, affected products or versions, and relevant third-party components;
- coordinate with relevant suppliers or component manufacturers when appropriate;
- develop or obtain appropriate corrective or mitigating measures; and
- provide appropriate status information to the reporter and notify affected customers, authorities, or other parties when required or appropriate.

The time required to investigate and remediate a vulnerability will vary depending on its complexity, severity, affected products, availability of corrective measures, and the involvement of third-party suppliers. HIS will handle vulnerability reports in a manner intended to protect sensitive cybersecurity information and may share relevant information with suppliers, service providers, cybersecurity specialists, customers, or authorities when necessary to investigate, remediate, disclose, or report the vulnerability.

Cybersecurity Updates and Disclosure

HIS will address validated vulnerabilities according to their cybersecurity risk and applicable legal requirements. Corrective measures may include software or firmware updates, configuration changes, hardware modifications, replacement components, customer advisories, or other appropriate mitigations.

For CRA-covered products, HIS will provide cybersecurity updates and information about fixed vulnerabilities in accordance with applicable CRA requirements throughout the applicable cybersecurity support period. HIS may delay detailed public disclosure when justified by cybersecurity risk and permitted by applicable law. Where required, HIS will also make applicable regulatory notifications concerning actively exploited vulnerabilities or severe cybersecurity incidents.