Coordinated Vulnerability Disclosure (CVD) Policy

Reporting security vulnerabilities in Instron Corporation products

This policy describes its scope, how to report a vulnerability to us, what you can expect from us, what we expect from reporters, secure communication options, and how we handle disclosure including publication and recognition.

Scope

This policy applies to security vulnerabilities in Instron Corporation products and associated services. Some products carry additional regulatory obligations (e.g., the EU Cyber Resilience Act); where they do, those obligations also apply. Instron's Product Security Team determines the in-scope products by conducting product-by-product scoping analysis.

How to Report a Vulnerability

You can report a vulnerability, and provide secure communication options for future correspondence, through any of the following channels. To meet accessibility needs, we offer the following methods of secure communication:

- Web: https://instronservice.com/GuestUser/Support
- Phone: (US) +1-781-828-2500 (Only available during business hours)

All communication channels used to exchange vulnerability details are secure. Where sensitive information is shared, we use encrypted email signed with S/MIME or OpenPGP, or another ISO-approved secure method, to prevent potentially critical information from being leaked.

What to Include

To help us investigate efficiently, please include as much of the following as you can:

- Affected product name, model number, and firmware/software version affected
- Description of the vulnerability and its potential impact
- Step-by-step reproduction instructions, proof-of-concept code, or scripts (if available)
- Whether you believe the vulnerability is being actively exploited
- Your preferred (secure) contact method
- Whether you would like to be credited for the discovery

What to Expect From Us

Acknowledgment and Communication

We aim to acknowledge your report within 3 business days and provide a reference for future correspondence. We will communicate with you using the secure communication options above, including during the investigation and remediation stages, and will reach out using these secure channels if we need more information.

Coordinated Vulnerability Disclosure (CVD) Policy

Remediation Timelines

We prioritize remediation based on assessed severity and risk. We aim to address vulnerabilities without undue delay, considering the complexity of the fix, any required coordination with upstream suppliers, and the need to test changes before release.

Embargo and Disclosure

We do not disclose vulnerability details before a fix or adequate mitigation is available, except where active exploitation necessitates early advisory guidance to protect affected users. We will inform you of the progress towards resolving the problem and whether we will issue a public advisory. To discuss the disclosure timeline, contact us through a secure reporting channel.

Actively exploited vulnerability: If we confirm active exploitation, we will issue an early advisory with mitigation guidance while the full fix is in development.

Third-party component vulnerability: If the reported vulnerability originates in an upstream component, we will engage the supplier and coordinate remediation. We will keep you informed of progress and any impact on the expected timeline.

Public Advisory

Once a fix is available and users have had an opportunity to update, we publish a public advisory that includes: a description of the vulnerability, affected product versions, severity and impact, remediation guidance, and credit to the reporter (if desired). Security updates addressing vulnerabilities are provided free of charge.

What We Ask of Reporters

We ask that you act in good faith:

- Give us reasonable time to investigate and remediate before any public disclosure.
- Do not reveal the problem to others until it has been resolved.
- Do not exploit the vulnerability beyond what is necessary to demonstrate it — this includes not accessing, modifying, or deleting data belonging to other users.
- Do not degrade or disrupt services (e.g., denial of service testing).
- Do not use attacks on physical security, social engineering, distributed denial of service, spam, or applications of third parties.
- Comply with applicable laws during your research.

EU Cyber Resilience Act Compliance

Certain Instron Corporation products sold in the European Union are subject to the EU Cyber Resilience Act (CRA), where applicable. In-scope products are determined by product-by-product scoping analysis. For in-scope products, we comply with the applicable vulnerability handling and reporting obligations of the CRA, where applicable, including obligations to notify relevant authorities when actively exploited vulnerabilities are identified.