Buehler, An ITW Company
Worldwide Headquarters
41 Waukegan Road, Lake Bluff, Illinois, 60044 USA
+1.847.295.6500 | 800-BUEHLER
info@buehler.com
www.buehler.com

Coordinated Vulnerability Disclosure (CVD) Policy

Version: 1.0 | Effective: September 11, 2026

Reporting Security Vulnerabilities in Buehler Products

This policy describes the scope of Buehler's coordinated vulnerability disclosure process including 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.

In-Scope Products

This Policy applies to all products with digital elements (including embedded software, firmware, or networked functionality) manufactured or distributed by Buehler in the European Union, including but not limited to the following products: AbrasiMet L Pro, AbrasiMet XL Pro, AutoMet, DiaMet, EcoMet 30, IsoMet High Speed, OmniMet, SimpliVac, Wilson Hardness Testers.

Scope is limited to products currently in production or in active support, as defined in the applicable product support policy for each product line.

Out-of-Scope

This Policy does not cover:

- Buehler corporate websites, IT infrastructure, email systems, and administrative networks;
- End-of-life products, except where actively exploited and reported within 12 months of support ending;
- Denial-of-service attacks, social engineering, or attacks requiring physical access;
- Previously disclosed or publicly known vulnerabilities.

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://www.buehler.com/contact-us.php
- Email: support@buehler.com
- Phone: +1-847-295-6500

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 in the wild
- Your preferred (secure) contact method
- Whether you would like to be credited for the discovery

What to Expect From Us

Acknowledgment and Communication

We will 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.

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 publicly 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).

Buehler, An ITW Company • Worldwide Headquarters

41 Waukegan Road, Lake Bluff, Illinois, 60044 USA | **phone:** 847.295.6500 • 800-BUEHLER | **email:** info@buehler.com

www.buehler.com

Buehler, An ITW Company
Worldwide Headquarters
41 Waukegan Road, Lake Bluff, Illinois, 60044 USA
+1.847.295.6500 | 800-BUEHLER
info@buehler.com
www.buehler.com

- 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 Buehler 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.

Buehler, An ITW Company • Worldwide Headquarters

41 Waukegan Road, Lake Bluff, Illinois, 60044 USA | **phone:** 847.295.6500 • 800-BUEHLER | **email:** info@buehler.com

www.buehler.com