KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Vulnerability Disclosure Policy

This Vulnerability Disclosure Policy (abbreviated “VDP”) is intended to give finders of potential security issues (“you”) clear guidelines for identifying and reporting potential security issues to KRONES. “Security issues” include publicly-known security vulnerabilities (e.g., with assigned CVE ID) and misconfiguration.

Scope of this VDP

Public IT systems (web applications, websites) by KRONES

This VDP applies to the following public IT systems (web applications, websites) by KRONES:

www.krones.com
blog.krones.com
www.steinecker.com
www.kic-krones.com
www.evoguard.com
www.ecomac.de
www.milkron.com
www.dekron.tech
www.kosme.com
www.hst-homogenizers.com
www.krones-izumi.com
www.konplan.cz
www.javlyn.com
craftbrewing.krones.com
www.kroki-neutraubling.de
www.bevkeg.com
www.unicornindustries.in
service.krones.eu
www.krones.ae
www.krones.co.th
www.kronesusa.com
www.ampcopumps.com
www.mht-ag.de
www.ipsplastics.com
www.systemlogistics.com
www.rdcustomautomation.com
www.gernep.de
www.sprinkman.com
www.transmarket.com
www.processanddata.com
*.share2act-dev.io
*.share2act-test.io
*.share2act.io
*.krones.digital
*.triacos.com
*.syskron.com

Any IT system not expressly listed above **is excluded from the scope of this VDP**.

If you aren’t sure whether an IT system is in scope or not, e-mail cyber.security@krones.com before starting any activities.

Products manufactured by KRONES and offered by KRONES to customers

Additional to the public IT systems listed above, this VDP also applies to all products manufactured by KRONES and offered by KRONES to its customers, such as entire machines and Manufacturing Execution Systems.

Third-party products, parts, and components that aren't manufactured by KRONES **are excluded from the scope of this VDP.**

If you aren't sure whether a product, part, or component is in scope or not, e-mail cyber.security@krones.com before starting any activities.

Authorization for testing

- **If at any time you have concerns or are uncertain whether your activities are consistent with this VDP, e-mail cyber.security@krones.com before going any further.**
- Testing the security of KRONES products in scope of this VDP **may require special permits** by KRONES, its customers, its suppliers, or other parties. If you aren't sure whether a permit is required, e-mail cyber.security@krones.com before starting any activities.

Prohibited types of testing

Do not conduct any kind of testing that affects the availability of KRONES services, modifies or deletes data of KRONES, modifies or affects security measures of KRONES, or is legally prohibited. **Especially prohibited are any kind of:**

- Denial-of-service testing
- Brute-force testing
- Social engineering, including phishing and impersonation attacks
- Testing that requires bypassing physical access control without permit
- Testing that includes uploading or executing code or software written by you or third parties
- Testing to compromise KRONES user accounts
- Testing to read, unmask, copy, steal, etc. any private credentials, including passwords and private keys

Requirements on testing

- **Do not test anything out of scope of this VDP.** If you aren't sure whether something is in scope of this VDP or not, e-mail cyber.security@krones.com before starting any activities.
- **Limit the amount of data you access to the minimum** required for demonstrating a proof of concept. If you encounter any personal data, proprietary information, or other sensitive data, stop testing and submit your report immediately. **Do not download or share any sensitive data.**
- **Do not disclose any potential security issues** to third parties, including the public internet, before KRONES resolved the potential issue.
- **Do not engage in extortion and unprofessional behavior.** Do not repeatedly ask for "bug bounties," payment, or other compensation that KRONES and you didn't agree on before you started any activities. Do not send the same report numerous times, including changing the sender e-mail address.

Identifying and reporting a potential security issue to KRONES

1. Test IT systems and products in the scope of this VDP as required. Always meet the requirements of this VDP.
2. Write your report:
   a. List the affected IT system (e.g., IP address, FQDN) or product (e.g., product name, commissioning number).
   b. Describe the potential security issue (e.g., type, class, CWE ID, CVE ID).
   c. Include a step-by-step guide that helps KRONES to reproduce the issue you identified.
3. Send your report to cyber.security@krones.com only. Add a proof of concept and screenshots if crucial to understand your report. Encrypt your report and attachments with the KRONES OpenPGP key. You may send your report anonymously. Provide your OpenPGP key if encrypted communication is required.
4. KRONES will analyze your report and confirm its receival within three business days (Germany).
5. KRONES will discuss further steps to resolve existing issues if your report is valid, not a duplicate, and meets the requirements as stated in this VDP.

Excluded, non-valid issues

The following set of “issues” is excluded from this VDP on purpose. While you can still send your report to cyber.security@krones.com, KRONES will likely not change the current status.

- Missing HTTP response headers that are considered “legacy” by the cyber security community or are widely unsupported by recent and current web browsers.
- Client-side issues, such as misconfiguring a client-side web browser to use a non-default configuration that may result in insecure access to KRONES IT systems.
- Unprocessed, raw results of vulnerability scanning tools and scripts.

Changes to this Vulnerability Disclosure Policy

KRONES reserves the right to update and improve this VDP. Please always consider the current version of the VDP.