

Kobold Messring GmbH

Vulnerability Disclosure Policy



Product Security

Vulnerability Disclosure Policy

At KOBOLD, the security and reliability of our products are an integral part of the trust our customers place in us. We therefore welcome reports of potential security vulnerabilities from customers, security researchers, partners, CERTs and other third parties. Through our Coordinated Vulnerability Disclosure (CVD) program, such reports help us identify potential weaknesses and continuously improve the security of our products.

We investigate reported vulnerabilities carefully and are committed to addressing confirmed security issues in a timely and responsible manner, working constructively with reporting parties and relevant stakeholders.

To protect our customers and avoid unnecessary security risks, we encourage coordinated disclosure. We ask reporting parties to allow us reasonable time to investigate reported issues, assess their potential impact and, where necessary, develop appropriate corrective measures before information is made publicly available.

If you discover a potential security vulnerability affecting a KOBOLD product, please report it using the channels provided below. KOBOLD will work in good faith with reporting parties who avoid privacy violations, data destruction, service disruption or other harmful activities and allow reasonable time for investigation and remediation.





Vulnerability Disclosure Policy

► Scope

This Vulnerability Disclosure Policy applies to cybersecurity vulnerabilities affecting products with digital elements marketed under the KOBOLD brand, including their associated software and firmware for which KOBOLD is responsible.

In Scope

- Kobold Messring products (e.g., hardware components, embedded software, Software tools).
- Kobold Messring digital infrastructure (e.g., websites, Service spots)

Outside of Scope (non-exhaustive)

- Third-party products, marketed by KOBOLD Messring but not under the KOBOLD brand.
- Products marketed by companies within the KOBOLD Group other than KOBOLD Messring.
- Vulnerabilities in third-party software, libraries or components that do not specifically affect a KOBOLD product.
- General product quality issues, functional defects, warranty claims and technical support requests that are not related to cybersecurity.
- Physical security issues that do not involve a cybersecurity vulnerability.
- Social engineering, phishing, vishing or other activities directed at KOBOLD employees.
- Denial-of-service, destructive or any testing that may impair the availability or operation of KOBOLD products.
- Vulnerabilities in customer networks or systems that are not under KOBOLD's control.

We welcome reports concerning vulnerabilities that may affect the security, integrity or intended operation of our products. Where you are unsure whether a potential vulnerability falls within the scope of this policy, you are welcome to submit the report and our PSIRT team will assess it.

Vulnerabilities affecting KOBOLD websites, IT systems or other corporate infrastructure are not handled through the Product Security reporting process and should be reported through our general security reporting channel: CSIRT@Kobold.com



Vulnerability Disclosure Policy

► Report a Vulnerability

To report a discovered or potential vulnerability in a KOBOLD product, send an email to:

PSIRT@kobold.com.

For a potential vulnerability in the KOBOLD Website, Infrastructure or online services, please send an email to:

CSIRT@kobold.com

Please include as much of the following information as possible.

- Type of Vulnerability; Product / Infrastructure
- Name/contact details — optionally anonymous where appropriate
- Affected product / system
- Product/firmware/software version, or URL/IP/Host, where applicable and if known
- Description of the suspected vulnerability and how it was discovered
- Steps to reproduce it, if available
- Supporting files/screenshots/logs, if available
- Whether you believe exploitation has already occurred
- Whether the vulnerability has been disclosed elsewhere (publicly?)
- Your preferred means of communication

To communicate large amounts of data, we shall provide you with an upload link

You may compose your report either in English or German. Unfortunately, we cannot guarantee a response for reports composed in other languages.

We shall respond within one business day upon receiving your email.

If you do not receive a response from us within one business day, please contact us again.



Vulnerability Disclosure Policy

► Handling Process



Upon receiving your report, the case will be logged with a unique tracking ID in our vulnerability register and the KOBOLD PSIRT team will be alerted. We will acknowledge receipt of the report within five working days and may contact the reporting party if additional information is required.

Based on the information provided, the reported security issue will be validated and assessed with regard to the affected product(s), exploitability, severity and potential impact. Where appropriate, we will attempt to reproduce the vulnerability and determine a suitable security fix, mitigation or other corrective action.

Once a corrective action has been determined, the remediation will be tested to confirm that the vulnerability has been adequately addressed without introducing unacceptable regressions.

Upon completion of our analysis, the KOBOLD PSIRT team will inform the reporting party of the outcome. Where appropriate, we will coordinate the remediation and disclosure process with the reporting party. If public disclosure is necessary, KOBOLD may publish a security advisory identifying the affected products and providing relevant information on the vulnerability, its severity, and available remediation or mitigation measures.

► Security Advisories

KOBOLD publishes security advisories where information about a confirmed vulnerability is relevant to the secure use of our products. Advisories may include information on affected products and versions, severity, available updates, mitigations and recommended actions.

► Security Advisories

There are currently no published KOBOLD Security Advisories.