Scope of this VDP

This Vulnerability Disclosure Policy (VDP) applies to KHS GmbH products containing digital elements. It aims to provide both vulnerability discoverers and customers operating KHS products with clear guidelines for reporting actively exploited vulnerabilities in KHS products and critical security incidents affecting KHS products.

Vulnerabilities in KHS products that are not actively exploited are handled via a separate standard process and are not covered by this policy. Third-party products, parts, and com-ponents that aren't manufactured by KHS are excluded from the scope of this VDP.

Definitions

Actively exploited vulnerability:

A vulnerability in a product with digital elements for which there is reliable information indicating that it is being or has been exploited by an attacker to carry out a cyberattack or to compromise the confidentiality, integrity, or availability of the product, its functions, or the information it processes.

Serious security incident:

A security incident (e.g., an attack on the operator's IT systems) that actually compromises, or has the potential to compromise, the security of a KHS product with digital elements and that results, or could result, in a significant impairment of the confidentiality, integrity, au-thenticity, or availability of the product, its functions, its security mechanisms, or the data processed by it.

Reporting channel

Reports regarding actively exploited vulnerabilities or serious security incidents can be sub-mitted either via email to the KHS Helpdesk or using the contact form on the Security Advi-sories page of the KHS website.

E-Mail: helpdesk@khs.com

KHS Homepage Contact Form: https://www.khs.com/security-advisories

Reaction targets

KHS defines the following response targets:

- Automatic acknowledgment of receipt: immediate
- Human acknowledgment: within 2 working days
- Triage: within 5 working days
- Status updates: at least every 10 working days
- Coordinated disclosure: generally, within 90 days (adjustable based on risk).

Rules of Engagement

Only good-faith security research within the scope of this policy is permitted. Specifically pro-hibited are DoS/DDoS attacks, social engineering, physical access, data exfiltration be-yond what is necessary for proof of concept (PoC), the modification or deletion of data, and the disruption of production, OT, or safety systems.

Disclosure & Data Proection

KHS discloses actively exploited vulnerabilities in a coordinated manner and publishes se-curity advisories regarding them; the identity of reporters is protected and disclosed only with their consent. Personal data is processed in accordance with the principle of data min-imization; please do not transmit sensitive data beyond what is necessary.

Disclaimer of Liability

KHS intends not to initiate legal action, provided this policy is adhered to in good faith and to the extent permitted by law and contract. This does not constitute a blanket waiver of legal rights and is not binding on third parties or authorities.