Geltungsbereich

Diese Richtlinie zur Offenlegung von Schwachstellen (kurz VDP) gilt für Produkte mit digitalen Elementen der KHS GmbH. Sie soll sowohl Findern von Schwachstellen als auch Kunden, die KHS Produkte betreiben, klare Vorgaben für die Meldung von aktiv ausgenutzten Schwachstellen an KHS Produkten und kritischen Sicherheitsvorfällen mit Auswirkung auf KHS Produkte an die Hand geben.

Nicht aktiv ausgenutzte Schwachstellen in KHS Produkten werden über einen separaten Regelprozess abgewickelt und sind nicht Gegenstand dieser Policy.

Produkte von Drittanbietern (Handelswaren), die von einem externen Hersteller in Verkehr gebracht wurden und von KHS ohne wesentliche Änderung in KHS-Anlagen eingesetzt werden, sind vom Geltungsbereich dieser VDP ausgenommen.

Definitionen

Aktiv ausgenutzte Schwachstelle:
Eine Schwachstelle in einem Produkt mit digitalen Elementen, für die belastbare Informationen vorliegen, dass sie durch einen Angreifer tatsächlich zur Durchführung eines Cyberangriffs oder zur unautorisierten Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit des Produkts, seiner Funktionen oder der von ihm verarbeiteten Informationen genutzt wird oder genutzt wurde.

Schwerwiegender Sicherheitsvorfall:
Ein Sicherheitsvorfall, der Auswirkungen auf die Sicherheit eine KHS Produkts mit digitalen Elementen hat, gilt als schwerwiegend, wenn

a) er sich negativ auf die Fähigkeit eines Produkts mit digitalen Elementen auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von sensiblen oder wichtigen Daten oder Funktionen zu schützen, oder

b) er zur Einführung oder Ausführung eines böswilligen Codes in einem Produkt mit digitalen Elementen oder im Netzwerk und Informationssystem eines Nutzers des Produkts mit digitalen Elementen geführt hat oder dazu führen kann.

Meldeweg

Die Meldung von aktiv ausgenutzten Schwachstellen bzw. schweren Sicherheitsvorfällen kann entweder über E-Mail an den KHS Helpdesk oder über das Kontaktformular auf der Security Advisories Seite der KHS Homepage erfolgen.

E-Mail: helpdesk@khs.com

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

Reaktionsziele

KHS definiert folgende Reaktionsziele:

- Automatische Eingangsbestätigung: sofort
- menschliche Bestätigung: binnen 2 Arbeitstagen
- Triage: binnen 5 Arbeitstagen
- Statusupdates: mindestens alle 10 Arbeitstage
- koordinierte Veröffentlichung: grundsätzlich innerhalb von 90 Tagen (risikobasiert anpassbar).

Rules of Engagement

Erlaubt ist ausschließlich gutgläubige Sicherheitsforschung im Rahmen dieser Richtlinie. Untersagt sind insbesondere DoS/DDoS, Social Engineering, physischer Zugriff, Datenexfiltration über einen notwendigen PoC hinaus, Änderung/Löschung von Daten sowie Störung von Produktions-, OT- oder Safety-Systemen.

Offenlegung & Datenschutz

KHS legt aktiv ausgenutzte Schwachstellen koordiniert offen und veröffentlicht dafür Security Advisories; die Identität von Meldern wird geschützt und nur mit Einwilligung genannt. Personenbezogene Daten werden datensparsam verarbeitet; bitte keine sensiblen Daten über das Erforderliche hinaus übermitteln.

Haftungshinweis

KHS beabsichtigt, bei gutgläubiger Einhaltung dieser Richtlinie keine rechtlichen Schritte einzuleiten, soweit gesetzlich und vertraglich zulässig. Dies ist kein pauschaler Rechtsverzicht und bindet keine Dritten oder Behörden.