

FERAG AG

Product Security Incident Response Team

Vulnerability Handling & Disclosure Process

Version	1.0
Datum	September 2026
Status	Freigegeben

Ferag AG

psirt@ferag.com

www.ferag.com/security

Industriestrasse 1, 8340 Hinwil, Schweiz

1 Ferag PSIRT – Vulnerability Handling & Disclosure Process

1.1 Einleitung

Ferag AG nimmt Sicherheitsbedenken ernst und arbeitet daran, diese schnell zu evaluieren und zu beheben. Das Ziel des Ferag Product Security Incident Response Teams (PSIRT) ist es, das Risiko für Kunden durch Sicherheitslücken zu minimieren – durch zeitnahe Information, Orientierung und Behebung von Schwachstellen in unseren Produkten, einschliesslich Software und Firmware.

Das Ferag PSIRT ist das zentrale Team innerhalb der Ferag AG für die Koordination der Untersuchung und Offenlegung von Sicherheitslücken. Alle Meldungen über mögliche Schwachstellen oder sicherheitsrelevante Vorfälle in Verbindung mit Ferag-Produkten können an das Ferag PSIRT weitergeleitet werden.

Sobald eine Meldung eingegangen ist, stellen wir die notwendigen Ressourcen bereit, um das Problem zu analysieren, zu validieren und Korrekturmassnahmen zu ergreifen. Das Ferag PSIRT koordiniert die Kommunikation mit allen Beteiligten – intern wie extern – um angemessen auf identifizierte Sicherheitsprobleme reagieren zu können.

Der Vulnerability Handling & Disclosure Process besteht bei Ferag aus vier Schritten (Abbildung 1):

1 Report	2 Analyse	3 Handling	4 Disclosure
Meldung eingehender Schwachstellen via E-Mail oder Formular	Validierung, Klassifizierung nach Security Impact Rating (SIR)	Interne Koordination, Entwicklung von Fixes oder Workarounds	Veröffentlichung via Security Advisory oder Release Notes

Abbildung 1: Ferag PSIRT – Vier-Stufen-Prozess

1.2 Zweck

Dieses Dokument wurde zur Information und Orientierung von Kunden, Sicherheitsforschern und Partnern erstellt, die eine Sicherheitslücke in einem Ferag-Produkt oder -Dienst melden möchten. Es soll sicherstellen, dass alle Beteiligten eine konsistente und eindeutige Grundlage haben, um zu verstehen, wie Ferag auf solche Ereignisse reagiert.

Dieses Dokument entspricht den Anforderungen von ISO/IEC 29147:2018 (Vulnerability Disclosure) und dem EU Cyber Resilience Act (CRA), Artikel 14 (Meldepflichten), sowie den Empfehlungen des BSI TR-03183 Teil 3.

1.3 Geltungsbereich

Diese Policy gilt für alle Ferag-Produkte und -Dienstleistungen mit digitalen Elementen, darunter:

- ferag.skyfall – Overhead-Fördersysteme und Pouch-Sorter
- ferag.skysort – Schalen-Sortiersysteme
- ferag.skymove – Fördersysteme
- Ferag.doWarehouse – WMS/WES/SCADA-Software
- Alle zugehörigen PLC-Steuerungen, HMIs, Firmware und Embedded-Systeme
- Alle weiteren Ferag-Produkte, die Software oder Firmware enthalten

Die Policy gilt unabhängig vom Servicevertrags- oder Produktlebenszyklus-Status des betroffenen Produkts.

1.4 Meldung (Report)

Jeder ist eingeladen, entdeckte Sicherheitslücken zu melden – unabhängig von Serviceverträgen oder dem Lebenszyklusstatus des Produkts. Ferag begrüsst Schwachstellenmeldungen von Sicherheitsforschern, Industriegruppen, CERTs, Partnern und allen anderen Quellen.

Ferag verlangt **keine Geheimhaltungsvereinbarung (NDA)** als Voraussetzung für die Entgegennahme von Meldungen.

Ferag respektiert die Interessen der meldenden Partei und verpflichtet sich, jede Schwachstelle, die nach vernünftigem Ermessen mit Ferag-Produkten zusammenhängt, zu behandeln.

Ferag bittet meldende Parteien dringend, eine **koordinierte Offenlegung** durchzuführen, da eine sofortige öffentliche Offenlegung eine „0-Day-Situation“ erzeugt, die Ferag-Kunden unnötig gefährdet.

1.4.1 Kontaktwege

Um eine Sicherheitslücke in einem Ferag-Produkt zu melden, kontaktieren Sie bitte das Ferag PSIRT:

Kanal	Kontakt / URL
E-Mail	psirt@ferag.com
Webformular	https://www.ferag.com/security/report

Bitte geben Sie mit Ihrer Meldung folgende Informationen an:

- Beschreibung der Schwachstelle, inkl. Proof-of-Concept-Exploit-Code oder Netzwerk-Traces (falls verfügbar)
- Betroffenes Produkt inkl. Seriennummer / Anlagenummer
- Öffentlichkeitsstatus der Schwachstelle (wurde sie bereits öffentlich disclosed?)
- Einverständnis zur namentlichen Nennung in einem Security Advisory (falls gewünscht)

1.4.2 Umgang mit Kontaktdaten der Melder

Wenn das Ferag PSIRT eine Schwachstellenmeldung erhält, die als schwerwiegend eingestuft wird, werden die Kontaktdaten des Melders – sofern nicht bereits vorhanden – in einer internen Melderdatenbank erfasst. Die Verwaltung dieser Daten erfolgt gemäss den Anforderungen der DSGVO (Datenschutz-Grundverordnung).

Die Kontaktdaten werden ausschliesslich verwendet, um mit dem Melder in Kontakt zu treten und zu kommunizieren. Darüber hinaus können sie auf ausdrücklichen Wunsch des Melders im Security Advisory oder in einem Hall of Fame genannt werden.

Kontaktdaten von Meldern, mit denen seit mehr als 3 Jahren keine Kommunikation stattgefunden hat, werden gelöscht.

1.4.3 Bug Bounty

Das Ferag PSIRT verfügt derzeit über kein Bug-Bounty-Programm. Meldende Parteien können jedoch auf ausdrücklichen Wunsch im Ferag Security Advisory als Entdecker genannt werden. Diese Einwilligung kann jederzeit in Übereinstimmung mit der DSGVO widerrufen werden.

1.5 Analyse und Verifizierung

Ferag untersucht und analysiert die Gültigkeit der gemeldeten Schwachstelle. Die Relevanz und der Bezug zu Ferag-Produkten werden verifiziert. Falls erforderlich, fordert Ferag weitere Informationen vom Melder an.

Während der Analysephase hält das Ferag PSIRT regelmässig Kontakt zur meldenden Partei, um über den aktuellen Status zu informieren und sicherzustellen, dass der Standpunkt des Melders verstanden wird.

1.5.1 Klassifizierung von Schwachstellen

Ferag bewertet und klassifiziert Schwachstellen anhand des Security Impact Rating (SIR) – einer qualitativen Einstufung, die eine angemessene Priorisierung im Schwachstellenmanagement ermöglicht:

Security Impact Rating (SIR)	Beschreibung
Kritisch	Schwachstelle ermöglicht vollständige Systemkompromittierung ohne Authentifizierung
Hoch	Erhebliche Auswirkungen auf Vertraulichkeit, Integrität oder Verfügbarkeit
Mittel (Standard)	Eingeschränkte Auswirkungen; Ferag weist standardmässig dieses Rating zu bis zur vollständigen Analyse
Niedrig / Informativ	Minimale Auswirkungen; kein unmittelbarer Handlungsbedarf

Bei Schwachstellen in Drittanbieter-Softwarekomponenten, die in Ferag-Produkten verwendet werden, leitet das Ferag PSIRT das SIR aus dem vom Komponentenhersteller bereitgestellten CVSS-Score ab und passt es an den Ferag-spezifischen Kontext an. Dabei werden folgende Faktoren berücksichtigt:

- Die potenzielle Auswirkung der Schwachstelle auf Ferag-Produkte und Kundensysteme
- Öffentlicher Bekanntheitsgrad der Schwachstelle
- Existenz und Verfügbarkeit von publizierten Exploits
- Anzahl der betroffenen, im Einsatz befindlichen Produkte
- Verfügbarkeit einer wirksamen Minderungsmassnahme anstelle eines Patches

1.6 Handling

Ferag führt die interne Schwachstellenbehandlung in Zusammenarbeit mit den verantwortlichen Entwicklungsteams durch. Während dieser Phase wird regelmässige Kommunikation zwischen Ferag und der meldenden Partei aufrechterhalten, um über den aktuellen Status zu informieren.

Falls verfügbar, können Vorabversionen von Software-Fixes und Ferag Security Advisories der meldenden Partei zur Verifikation zur Verfügung gestellt werden.

1.6.1 Arten der Behebung (Remediation)

Nachdem eine Schwachstelle erfolgreich analysiert wurde und ein Fix erforderlich ist, werden entsprechende Korrekturen entwickelt und zur Verteilung vorbereitet. Die Reaktionszeiten hängen von verschiedenen Faktoren ab, darunter die Schwere der Schwachstelle, das betroffene Produkt, der aktuelle Entwicklungszyklus und die QA-Prozesse.

Eine Behebung kann eine oder mehrere der folgenden Formen annehmen:

- Ein neues Software- oder Firmware-Release
- Ein von Ferag bereitgestellter Patch oder eine neue Version der Software/Firmware
- Anweisungen zum Herunterladen und Installieren eines Updates oder Patches eines Drittanbieters
- Ein Workaround zur Minderung der Schwachstelle

Ferag garantiert keine spezifische Lösung für alle gemeldeten Probleme. Nicht alle identifizierten Schwachstellen können behoben werden.

1.7 Offenlegung (Disclosure)

Ferag verwendet Ferag Security Advisories und Software Release Notes für die Veröffentlichung von Schwachstellen. Die nachfolgende Tabelle zeigt die Publikationstypen abhängig vom Security Impact Rating:

Security Impact Rating (SIR)	CVE erforderlich	Publikationstyp
Kritisch	Ja	Ferag Security Advisory
Hoch	Ja	Ferag Security Advisory
Mittel (Standard)	Nein	Software Release Notes
Niedrig / Informativ	Nein	Software Release Notes

1.7.1 Ferag Security Advisory

Ferag Security Advisories liefern detaillierte Informationen zu Sicherheitsproblemen, die Ferag-Produkte direkt betreffen und eine Aktualisierung, einen Fix oder eine andere Kundenaktion erfordern. Sie werden für Schwachstellen mit einem SIR-Score von Hoch oder Kritisch veröffentlicht.

Ein Ferag Security Advisory enthält üblicherweise:

- Beschreibung der Schwachstelle mit CVE-Referenz und CVSS-Score
- Identität der bekannten betroffenen Produkte und Software-/Hardware-Versionen
- Informationen zu Minderungsfaktoren und Workarounds
- Ort der verfügbaren Fixes
- Mit Einverständnis der meldenden Partei: Anerkennung für die Meldung und Mitarbeit

1.7.2 Software Release Notes

Software Release Notes werden verwendet, um Probleme mit mittlerem und niedrigem/informativem Schweregrad zu veröffentlichen. Sie enthalten neue Informationen wie Versionsänderungen, neue Funktionen, behobene Fehler und CVE-IDs.

1.7.3 Kundenbenachrichtigung

Ferag beabsichtigt, Kunden zu benachrichtigen, sobald ein praktischer Workaround oder ein Fix für eine Sicherheitslücke identifiziert wurde. Die Benachrichtigung erfolgt nach Abschluss des Vulnerability-Handling-Prozesses.

Falls das Ferag PSIRT eine aktive Ausnutzung einer Schwachstelle beobachtet, wird Ferag die Veröffentlichung einer Sicherheitsmitteilung beschleunigen – auch wenn noch kein vollständiger Patch oder Workaround vorliegt.

Publikationstyp	E-Mail an Kunden	Ferag Supportportal
Ferag Security Advisory	Ja	Ja
Software Release Notes	Nein	Ja

1.8 Meldepflicht gemäss CRA (Art. 14)

Ab dem **11. September 2026** ist Ferag AG verpflichtet, aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle innerhalb von **24 Stunden** über die **ENISA Single Reporting Platform (SRP)** zu melden.

Das Ferag PSIRT ist verantwortlich für die fristgerechte Erfüllung dieser Meldepflicht.

Ereignis	Frist	Empfänger
Aktiv ausgenutzte Schwachstelle entdeckt	24 Stunden (Erstmeldung)	ENISA SRP
Detaillierter Bericht	72 Stunden	ENISA SRP
Abschlussbericht (falls kein Fix innert 14 Tagen)	Innerhalb 14 Tage	ENISA SRP

1.9 Definitionen

Begriff	Definition
PSIRT	Product Security Incident Response Team – Team, das für die Bearbeitung von Sicherheitsproblemen in Produkten oder Diensten verantwortlich ist.
Finder / Melder	Person, die eine potenzielle Sicherheitslücke in einem Ferag-Produkt entdeckt und meldet. Dazu gehören Sicherheitsforscher, Software-Ingenieure, Systemadministratoren und Kunden.
Report / Meldung	Beschreibung einer potenziellen Schwachstelle durch den Finder. Meldungen sind immer vertraulich und nicht öffentlich.
Schwachstelle	Ein Software- oder Firmware-Fehler, der einem Angreifer ermöglicht, eine Aktion in Verletzung einer Sicherheitsrichtlinie durchzuführen. Design-Fehler und Nichtbeachtung von Security-Best-Practices können ebenfalls als Schwachstellen gelten.
CVE	Common Vulnerabilities and Exposures – ein Verzeichnis öffentlich bekannter Cybersicherheits-Schwachstellen mit eindeutiger Kennnummer.
CVSS	Common Vulnerability Scoring System – standardisiertes Bewertungssystem für den Schweregrad von Schwachstellen (0.0–10.0).
SIR	Security Impact Rating – Ferag-interne qualitative Klassifizierung (Kritisch / Hoch / Mittel / Niedrig).
CVD	Coordinated Vulnerability Disclosure – koordinierte Offenlegung zwischen Melder und Hersteller vor öffentlicher Publikation.

Begriff	Definition
CRA	EU Cyber Resilience Act (Verordnung 2024/2847) – EU-Verordnung mit verbindlichen Cybersicherheitsanforderungen für Produkte mit digitalen Elementen.

2 Änderungshistorie

Version	Datum	Änderungen
1.0	September 2026	Erstveröffentlichung. Basierend auf Festo PSIRT VDP v1.2 als Referenz, angepasst an Ferag-Produkte und CRA-Anforderungen.