Prozessbeschreibung Vulnerability Handling

1 Einführung

Die Gewährleistung der Produkt- und Anlagensicherheit besitzt für INSEVIS höchste Priorität. Als Hersteller von Komponenten für die industrielle Automatisierungstechnik sind wir uns der Rolle unserer Produkte im Rahmen eines ganzheitlichen Sicherheitskonzepts von Maschinen und Produktionsanlagen bewusst.

Das vorliegende Dokument dient dem Zweck, unseren Ansatz für Sicherheitsvorfälle und Schwachstellen transparent darzulegen und die Zusammenarbeit mit unseren Kunden, Anwendern sowie Partnern nachhaltig zu stärken. INSEVIS bietet den Anwendern hiermit eine konsistente, eindeutige Informationsquelle, um das Vorgehen bei Sicherheitsereignissen verständlich zu machen und sie effektiv bei der Bewältigung von Sicherheitsrisiken zu unterstützen.

Das INSEVIS Product Security Incident Response Team (PSIRT) steuert dazu zentral das gesamte Schwachstellenmanagement. Das primäre Ziel des PSIRT ist es, potenzielle Risiken durch IT-Sicherheitslücken für unsere Kunden zu minimieren und die dauerhaft sichere Verwendbarkeit aller INSEVIS-Produkte, Softwarelösungen und Anwendungen zu garantieren. Das PSIRT fungiert als zentrale Instanz innerhalb des Unternehmens für die Untersuchung, Bewertung und Offenlegung von Sicherheitsrisiken. Es dient als zentraler Meldeeingang für sämtliche Hinweise auf potenzielle Schwachstellen oder Sicherheitsvorfälle im Zusammenhang mit INSEVIS-Produkten.

Nach dem Erhalt einer Meldung setzt das Team unverzüglich die erforderlichen Ressourcen ein, um das Problem zu analysieren, zu validieren und angemessene Abhilfemaßnahmen zu ergreifen. Zur Sicherstellung eines standardisierten Verfahrens arbeitet das INSEVIS PSIRT eng mit der Allianz **CERT@VDE** zusammen. Diese Kooperation gewährleistet eine koordinierte Reaktion und transparente Offenlegung (Coordinated Vulnerability Disclosure) aller extern identifizierten Produktschwachstellen.

Der strukturierte Schwachstellenbehandlungs- und Bekanntgabeprozess gliedert sich in die folgenden **vier Phasen**:

1. **Meldung (Report):** Sichere Entgegennahme und Erstregistrierung der Schwachstellenmeldung.
2. **Analyse:** Technische Validierung, Risikobewertung (z. B. via CVSS) und Ursachenforschung.
3. **Bearbeitung:** Entwicklung, Testung und Bereitstellung von Sicherheitsupdates, Patches oder Workarounds.
4. **Offenlegung (Disclosure):** Publikation von Sicherheitshinweisen (Advisories) und Hilfestellungen für betroffene Anwender.

2 Meldung (Report)

Der Prozess zur Meldung von Sicherheitslücken steht jeder Person oder Organisation uneingeschränkt offen. Eine Meldung ist unabhängig von bestehenden Vertragsverhältnissen, dem Lebenszyklusstatus des betroffenen Produkts (einschließlich End-of-Life-Produkten) oder dem Kundenstatus bei INSEVIS möglich.
INSEVIS begrüßt ausdrücklich Schwachstellenmeldungen von Sicherheitsforschern, Industriegruppen, CERTs, Partnern sowie allen weiteren externen Quellen. Der Erhalt von Meldungen setzt den Abschluss einer Geheimhaltungsvereinbarung (NDA) nicht voraus.
INSEVIS respektiert die Interessen der meldenden Partei, behandelt Meldungen auf Wunsch vollständig anonym und verpflichtet sich zur Untersuchung jeder Schwachstelle, bei der ein begründeter Zusammenhang mit INSEVIS-Produkten vermutet werden kann.
Zur Gewährleistung der Kundensicherheit bittet INSEVIS die meldenden Parteien dringend um ein koordiniertes Vorgehen (Coordinated Vulnerability Disclosure). Eine sofortige, unkoordinierte Veröffentlichung führt zu einer kritischen Zero-Day-Situation, welche die Anlagen und Systeme unserer Kunden unnötig gefährdet.
Zur Einreichung einer Schwachstellenmeldung, die ein Produkt von INSEVIS betrifft, stehen folgende Kontaktkanäle zum INSEVIS PSIRT zur Verfügung:

- **E-Mail:** psirt@insevis.de
- **Meldung über den Koordinationspartner CERT@VDE:** https://cert.vde.com
  Für eine effiziente Bearbeitung und Validierung wird um die Bereitstellung folgender Informationen gebeten:
- **Beschreibung der Schwachstelle:** Detailberichte inklusive Proof-of-Concept (PoC), Exploit-Code oder relevanten Netzwerkprotokollen (sofern verfügbar).
- **Produktidentifikation:** Genaue Angabe des betroffenen Produkts, des Modells sowie der Firmware-Version.
- **Aktueller Bekanntheitsgrad:** Informationen darüber, ob die Schwachstelle bereits öffentlich diskutiert oder publiziert wurde.
- **Nennung im Advisory:** Ausdrückliche Zustimmung oder Ablehnung (bzw. Wunsch nach anonymer Meldung) bezüglich einer namentlichen Erwähnung des Meldenden im Rahmen des offiziellen INSEVIS Security Advisory.

Die E-Mail-Kommunikation mit dem INSEVIS PSIRT kann verschlüsselt erfolgen. Die entsprechenden S/MIME- und PGP-Schlüssel sowie weiterführende Informationen zum PSIRT sind unter folgendem Link abrufbar https://www.INSEVIS.de/……../

2.1 Umgang mit den Kontaktdaten der Meldenden

Nach dem Eingang einer validierten Schwachstellenmeldung werden die Kontaktdaten der meldenden Partei – sofern noch nicht vorhanden – in die interne Meldedatenbank aufgenommen. Die Speicherung und Pflege dieser Daten erfolgt strikt nach den Bestimmungen der Datenschutz-Grundverordnung (DS GVO). Die Kontaktdaten dienen ausschließlich der direkten Kommunikation und Abstimmung mit dem Melder während des laufenden Prozesses. Kontaktdaten von Meldern, mit denen über einen Zeitraum von drei Jahren keine aktive Kommunikation mehr stattgefunden hat, werden gelöscht.

Weiterführende Informationen zum Datenschutz bei INSEVIS finden Sie unter https://www.INSEVIS.de/…….

3 Analyse und Verifizierung

Das INSEVIS PSIRT untersucht und analysiert jede eingehende Meldung systematisch. Diese Prüfung erfolgt unabhängig von der betroffenen Softwareversion oder dem aktuellen Status des Produktlebenszyklus, sofern das Produkt den definierten „Last Day of Support“ (LDoS) noch nicht erreicht hat.

Im ersten Schritt verifiziert INSEVIS die Relevanz sowie die konkrete Anwendbarkeit der gemeldeten Schwachstelle auf INSEVIS-Produkte. Sollten die vorliegenden Daten für eine eindeutige Validierung nicht ausreichen, fordert das PSIRT gezielt weitere technische Informationen bei der meldenden Partei an.

3.1 Klassifizierung von Schwachstellen

Zur Gewährleistung einer objektiven Bewertung und einer risikobasierten Priorisierung im Rahmen des Schwachstellenmanagementprozesses klassifiziert INSEVIS identifizierte Sicherheitslücken anhand eines qualitativen Bewertungsschemas (Niedrig, Mittel, Hoch, Kritisch).

Für eine fundierte Risikoeinstufung berücksichtigt INSEVIS standardmäßig die folgenden Parameter:

- **Potenzielle Auswirkungen:** Tragweite und Schadensausmaß der Schwachstelle auf die Integrität, Verfügbarkeit und Vertraulichkeit des Systems.
- **Öffentlicher Bekanntheitsgrad:** Aktueller Status des Wissens über die Sicherheitslücke in der Fachöffentlichkeit.
- **Exploit-Verfügbarkeit:** Nachweisbare Existenz oder Veröffentlichung von funktionalem Exploit-Code.
- **Betroffenheitsvolumen:** Anzahl und Verbreitung der im Feld eingesetzten INSEVIS-Produkte, welche diese Schwachstelle aufweisen.
- **Verfügbarkeit von Alternativen eines Patches:** Vorhandensein effektiver, temporärer Abhilfemaßnahmen (Mitigations) oder Workarounds als Übergangslösung bis zur Bereitstellung eines finalen Patches.

4 Bearbeitung

Die Behebung identifizierter Sicherheitslücken erfolgt durch das INSEVIS PSIRT in enger Abstimmung mit den zuständigen internen Entwicklungsgruppen. Als strategischer Partner wird das CERT@VDE frühzeitig über das Sicherheitsproblem informiert. Es unterstützt das INSEVIS PSIRT bei Bedarf bei der technischen Bewertung sowie bei der Ausarbeitung von offiziellen CVE-Einträgen (Common Vulnerabilities and Exposures) und Security Advisories.

Während der gesamten Bearbeitungsphase pflegt das INSEVIS PSIRT eine regelmäßige Kommunikation mit der meldenden Partei. Dies dient dem transparenten Austausch über den aktuellen Status und stellt sicher, dass die technische Position des Herstellers verstanden wird. Sofern zweckdienlich, können dem Melder Vorabversionen von Softwarekorrekturen oder Entwürfe der Sicherheitshinweise zur Verifizierung und Gegenprüfung zur Verfügung gestellt werden.

4.1 Abhilfemaßnahmen (Remediation)

INSEVIS untersucht Sicherheitsrisiken mit hoher Priorität und ist bestrebt, validierte Schwachstellen zeitnah zu patchen oder zu minimieren. Erfordert das Ergebnis der technischen Analyse eine Modifikation des Produkts, werden entsprechende Korrekturmaßnahmen entwickelt und für den Rollout vorbereitet.

Der Zeitplan für die Bereitstellung von Korrekturen ist von verschiedenen Faktoren abhängig. Dazu zählen die Kritikalität der Schwachstelle, das betroffene Produkt, der aktuelle Entwicklungszyklus, der Produktlebenszyklus sowie die Frage, ob eine Behebung ausschließlich im Rahmen eines Major-Releases (Hauptversion) realisiert werden kann.

Die bereitgestellten Abhilfemaßnahmen können folgende Formen annehmen:

- **Software-/Firmware-Release:** Veröffentlichung einer neuen, bereinigten Version der Software oder Firmware.
- **Patch/Update:** Bereitstellung einer gezielten Softwarekorrektur durch INSEVIS.
- **Drittanbieter-Instruktionen:** Handlungsanweisungen zur Installation von Updates oder Patches von Zulieferern und Drittanbietern.
- **Workaround:** Dokumentierte Maßnahmen zur wirksamen Abschwächung (Mitigation) der Schwachstelle ohne Code-Änderung.

Unabhängig von diesen Verfahrensweisen garantiert INSEVIS keine spezifische technische Lösung für jedes Problem. Es wird ausdrücklich darauf hingewiesen, dass unter Abwägung technologischer oder architektonischer Gegebenheiten nicht alle identifizierten Probleme vollständig behoben werden können.

5 Offenlegung (Disclosure)

Die Veröffentlichung validierter Schwachstellen erfolgt strukturiert über offizielle INSEVIS Security Advisories (Sicherheitshinweise) via CERT@VDE sowie über Software-Release-Notes (Versionshinweise) innerhalb der eigenen Kommunikationskanäle. Die Wahl des Publikationskanals richtet sich primär nach der Risikobewertung:

- **Schweregrad „Hoch“ oder „Kritisch“:** Für diese Schwachstellen publiziert INSEVIS grundsätzlich ein dediziertes Security Advisory über die Plattform des CERT@VDE.
- **Schweregrad „Niedrig“ oder „Mittel“:** Die Dokumentation und Offenlegung dieser Sicherheitslücken erfolgt standardmäßig im Rahmen der regulären Software-Release-Notes.

INSEVIS behält sich das Recht vor, im Einzelfall begründet von diesen Richtlinien abzuweichen, sofern zusätzliche Risikofaktoren eine alternative Handhabung erfordern.

5.1 CVE-Nummerierung

INSEVIS initiiert die Zuweisung einer CVE-Kennung (Common Vulnerabilities and Exposures), sofern eine verifizierte Schwachstelle direkt auf dem Quellcode oder einer spezifischen Implementierung von INSEVIS beruht. Die physische Vergabe der CVE-Nummer erfolgt über die zuständige CVE-Nummerierungsstelle (CNA) CERT@VDE.

CVE-Kennungen werden für gemeldete Schwachstellen erst dann final vergeben und publiziert, wenn die Sicherheitslücke durch INSEVIS in Abstimmung mit dem CERT@VDE offiziell bestätigt wurde oder diese nachweislich in einer verwendeten Komponente eines Drittanbieters existiert.

5.2 INSEVIS Sicherheitshinweis (Advisory)

INSEVIS Security Advisories stellen detaillierte technische Informationen über Sicherheitsrisiken bereit, die INSEVIS-Produkte direkt betreffen und ein Firmware-Upgrade, einen Software-Patch oder sonstige Kundenaktionen (z. B. die Implementierung eines Workarounds) erfordern. Die zentralen Publikationen werden auf der offiziellen Webseite des CERT@VDE bereitgestellt: `https://cert.vde.com/de/advisories/vendor/insevis`.

Ein INSEVIS Security Advisory enthält standardmäßig folgende Informationen:

- **Technische Beschreibung:** Detaillierte Darstellung der Sicherheitslücke inklusive CVE-Referenz und der konkreten CVSS-Klassifizierung.
- **Betroffenheitsmatrix:** Eindeutige Identifikation aller betroffenen Produkte, Modelle sowie Software- und Hardware-Versionen.
- **Mitigationen:** Umfassende Informationen zu abschwächenden Faktoren, Gegenmaßnahmen und temporären Workarounds.
- **Bezugsquellen:** Direkte Verweise und Links zum Download der bereitgestellten Firmware-Updates oder Patches.
- **Dank (Acknowledgement):** Vorbehaltlich des ausdrücklichen Einverständnisses wird die meldende Partei namentlich genannt, um deren Beitrag zur Erhöhung der Produktsicherheit zu würdigen.

5.3 Software-Freigabemitteilungen

Software-Release-Notes dienen der transparenten Dokumentation von korrigierten Schwachstellen mit niedrigem oder mittlerem Schweregrad. Über diese produktbegleitenden Dokumente erhalten Kunden alle relevanten Informationen zu Versionsänderungen, Funktionserweiterungen, behobenen Fehlern sowie gegebenenfalls zugehörigen CVE-IDs.

Die Bereitstellung der Release-Notes erfolgt direkt beim jeweiligen Produkt auf der INSEVIS-Webseite.

5.4 Kundenbenachrichtigung

INSEVIS ist bestrebt, Kunden proaktiv zu informieren, sobald eine funktionale Abhilfemaßnahme oder ein finaler Software-Fix für eine Sicherheitslücke identifiziert und verifiziert wurde. Für das Lifecycle- und Patch-Management greift INSEVIS auf etablierte Kundenbenachrichtigungsprozesse zurück. Diese können je nach Schweregrad die direkte Kundenansprache, die öffentliche Freigabe eines Security Advisory oder detaillierte Einträge in den Software-Release-Notes über CERT@VDE umfassen.

Diese Benachrichtigungen werden initiiert, nachdem das PSIRT den Schwachstellenbehandlungs- und Offenlegungsprozess erfolgreich abgeschlossen und das Vorhandensein valider Korrekturmaßnahmen oder koordinierter Release-Pläne zur Behebung der Schwachstellen bestätigt hat.

Sollte das INSEVIS PSIRT eine aktive Ausnutzung (Exploitation) einer Schwachstelle im Feld identifizieren, die zu einem akut erhöhten Risiko für INSEVIS-Kunden führt, wird die Veröffentlichung einer Sicherheitsmitteilung im Rahmen des Risikomanagements beschleunigt. Eine solche Sofortmitteilung enthält unter Umständen priorisierte Handlungsempfehlungen, auch wenn ein finaler Software-Patch zu diesem Zeitpunkt noch nicht zur Verfügung steht.

Zur Gewährleistung einer zielgerichteten und effektiven Informationspolitik nutzt INSEVIS – gesteuert nach dem jeweiligen Schweregrad der Schwachstelle – die folgenden primären Kommunikationswege:

- **Zentrale Publikation:** Offizielle Veröffentlichung von Security Advisories über die Plattform des CERT@VDE.
- **Newsletter-Verteiler:** Regelmäßige und anlassbezogene Updates für abonnierte Fach- und Kundenkreise.
- **Direktkommunikation:** Gezielte E-Mail-Benachrichtigungen an Kunden und Betreiber, die das spezifisch betroffene Produkt nachweislich bezogen haben.

Im Sinne einer optimalen Informationsbereitstellung behält sich INSEVIS das Recht vor, von Fall zu Fall strategische Ausnahmen von diesen Standardprozeduren zu machen, um die Transparenz und Reichweite der Kommunikation für ein bestimmtes Dokument situativ zu maximieren.