Security Incident & Vulnerability Report

Version 1.0 09/2026

NBB Controls + Components GmbH
Otto-Hahn-Straße 3 – 5 · 75248 Ölbronn-Dürrn · GERMANY · T: +49 7237 999-0 · F: +49 7237 999-199 · info@nbb.de · www.nbbcontrols.com
Registergericht Mannheim HRB 500961 · Geschäftsführer: Dipl.-Ing. Thomas Burchard, Dipl.-Wirtschafts-Ing. (FH) / MBA Pierre Augstein

Meldeformular für Cybersecurity-Vorfälle und Schwachstellen

Dringende Fälle:
Bitte senden Sie das ausgefüllte Formular an **security@nbb.de**. Bei akuter Gefährdung von Personen oder Anlagen ist die Anlage entsprechend den geltenden Betriebs- und Sicherheitsanweisungen in einen sicheren Zustand zu versetzen. Dieses Formular ersetzt keine Notfallmaßnahmen.

Interne Vorgangsnummer	
Eingangsdatum / Uhrzeit	

Zweck des Formulars

Dieses Formular dient Kunden, Betreibern, Integratoren, Sicherheitsforschenden und anderen externen Stellen zur strukturierten Meldung vermuteter oder bestätigter Cybersecurity-Schwachstellen und Sicherheitsvorfälle im Zusammenhang mit Produkten von NBB Controls+ Components GmbH (NBB).

Sicherheitshinweis:
Bitte keine Passwörter, privaten Schlüssel, Zugangstoken oder sonstigen Geheimnisse übermitteln. Potenziell schädliche, vertrauliche oder große Dateien nicht unaufgefordert per E-Mail senden, sondern zunächst beschreiben und einen sicheren Übertragungsweg mit **security@nbb.de** abstimmen.

Hinweis: Das Formular unterstützt die strukturierte Erfassung und interne CRA-Bewertung.
Ob im konkreten Fall eine gesetzliche Meldepflicht vorliegt, wird durch die Firma NBB bewertet.

1. Angaben zur meldenden Person

Name / Ansprechpartner	
Unternehmen / Organisation	
Funktion / Abteilung	
E-Mail-Adresse	
Telefonnummer	
Land	

Rolle der meldenden Person:

☐ Kunde / Betreiber
☐ Händler / Distributor
☐ Systemintegrator / Servicepartner
☐ Sicherheitsforscher/in
☐ Behörde / CSIRT
☐ Sonstige: _____

Bevorzugte Kontaktaufnahme:

☐ E-Mail
☐ Telefon

2. Art und Dringlichkeit der Meldung

Art der Meldung (Mehrfachauswahl möglich):

☐ Vermutete Schwachstelle
☐ Bestätigte Schwachstelle
☐ Vermutete aktive Ausnutzung
☐ Bestätigte aktive Ausnutzung
☐ Sicherheitsvorfall
☐ Verdächtiges Verhalten / Anomalie
☐ Sicherheitsproblem in Konfiguration / Dokumentation
☐ Sonstiges: _____

Vom Melder eingeschätzte Dringlichkeit:

☐ Kritisch
☐ Hoch
☐ Mittel
☐ Niedrig
☐ Unbekannt

Begründung der Dringlichkeit:
Bitte insbesondere laufende Angriffe, unmittelbare Gefährdungen oder großflächige Auswirkungen nennen.

3. Betroffenes Produkt

Produktart (Mehrfachauswahl möglich):

☐ Sender ☐ Empfänger

☐ Zubehör ☐ Konfigurations- oder Servicetool

☐ Firmware / Software ☐ Sonstiges: _____

Produktbezeichnung / Typ		
Artikelnummer		
Seriennummer(n)		
Hardware-Version		
Firmware-Version		
Software-/Tool-Version		
Konfigurationsstand / Projektdatei		

4. Betroffene Installation und Einsatzumgebung

Endkunde / Betreiber	
Standort / Land	
Anzahl betroffener Produkte	
Datum der Inbetriebnahme	

Betriebsstatus:

☐ Aktuell in Betrieb ☐ Außer Betrieb

☐ Vom Netzwerk / System getrennt ☐ Unbekannt

Einsatzkontext:

☐ Industrielle Maschine / Anlage ☐ Mobile Maschine / Fahrzeug

☐ Kran / Hebezeug ☐ Sonstige Anwendung: _____

Beschreibung der Systemumgebung:

Verbundene Systeme, Netzwerke, Schnittstellen, relevante Komponenten und Betriebsbedingungen.

5. Zeitlicher Verlauf und Entdeckung

Datum / Uhrzeit der Entdeckung	
Erstes bekanntes Auftreten	
Zeitzone	
Art der Entdeckung	

Chronologischer Ablauf:
Bekannte Ereignisse, Beobachtungen und Maßnahmen mit Datum und Uhrzeit in zeitlicher Reihenfolge.

6. Beschreibung des Vorfalls oder der Schwachstelle

Kurzbeschreibung:

Detaillierte Beschreibung:
Was ist passiert? Welches Verhalten wurde erwartet und welches tatsächlich beobachtet?

Betroffene Funktionen / Komponenten:
Zum Beispiel Funkkommunikation, CAN, Authentisierung, Update, Konfiguration, Diagnose oder Schutzfunktion.

7. Beobachtete oder mögliche Auswirkungen

Schutzziele / Funktionen:

☐ Verfügbarkeit beeinträchtigt
☐ Integrität beeinträchtigt
☐ Vertraulichkeit beeinträchtigt
☐ Authentizität beeinträchtigt
☐ Schadcode vermutet / bestätigt
☐ Unbefugter Zugriff vermutet / bestätigt
☐ Sicherheits- oder Schutzfunktion beeinträchtigt
☐ Keine Auswirkung festgestellt
☐ Unbekannt
☐ Sonstiges: _____

Ausmaß:

☐ Ein einzelnes Produkt
☐ Mehrere Produkte an einem Standort
☐ Mehrere Standorte / Kunden
☐ Umfang unbekannt

Beschreibung der tatsächlichen oder möglichen Auswirkungen:
Betroffene Daten, Funktionen, Betriebsunterbrechungen sowie mögliche Personen-, Sach- oder Umweltrisiken.

8. Hinweise auf aktive Ausnutzung

Liegen Hinweise auf aktive Ausnutzung vor?

☐ Ja, bestätigt
☐ Ja, vermutet
☐ Nein
☐ Unbekannt

Indikatoren / Begründung:
Zum Beispiel ungewöhnliche Zugriffe, Manipulationen, Schadcode, wiederkehrende Muster oder externe Hinweise.

Bekannte betroffene Organisationen / Systeme	
Öffentliche Veröffentlichung bekannt?	
Quelle / Referenz / CVE	

9. Technische Informationen

Möglicher Zugriffs- oder Angriffsweg:

☐ Funkverbindung
☐ Ethernet / Netzwerk
☐ Service- / Debug-Schnittstelle
☐ Update-Mechanismus
☐ Physischer Zugriff
☐ Sonstiges: _____

☐ CAN / Feldbus
☐ USB / lokaler Anschluss
☐ Konfiguration / Projektdatei
☐ Lieferkette / Drittkomponente
☐ Unbekannt

Technische Symptome, Fehlercodes und weitere Hinweise (z.B. Trace oder Log):

Vermutete Ursache oder Angriffsmethode:

Gerätekennungen, Adressen oder relevante Zeitstempel:
Nur angeben, soweit für die Untersuchung erforderlich und zur Weitergabe berechtigt.

10. Reproduzierbarkeit

Kann das Verhalten reproduziert werden?

☐ Ja, zuverlässig ☐ Ja, sporadisch ☐ Nein

☐ Nicht versucht ☐ Unbekannt

Voraussetzungen zur Reproduktion:

Schritte zur Reproduktion:
Bitte nummeriert. Keine Zugangsdaten oder Geheimnisse eintragen.

Beobachtetes Ergebnis / Erfolgsindikator:

11. Bereits durchgeführte Maßnahmen

☐ Produkt / Anlage außer Betrieb genommen
☐ Zugangsdaten geändert / widerrufen
☐ Konfiguration geändert
☐ Produkt ausgetauscht
☐ Kunden / Betreiber informiert
☐ Keine Maßnahmen
☐ Netzwerk- oder Systemverbindung getrennt
☐ Firmware / Software aktualisiert
☐ Produkt neu gestartet / zurückgesetzt
☐ Beweissicherung / Logs erstellt
☐ Behörde / CSIRT informiert
☐ Sonstiges: _____

Beschreibung der Maßnahmen und Ergebnis:
Datum/Uhrzeit, Verantwortliche und beobachtete Wirkung.

Noch bestehende Gefährdung oder Einschränkung:

12. Nachweise und Anhänge

☐ Screenshots / Fotos
☐ Konfigurationsdateien
☐ Video
☐ Proof of Concept / Reproduktionsskript
☐ Log-Dateien
☐ Netzwerk- oder Funkmitschnitte
☐ Diagnosebericht
☐ Sonstige Unterlagen

Liste und kurze Beschreibung der Anhänge:

Sicherer Austausch
Keine nicht erforderlichen personenbezogenen Daten oder Geheimnisse übermitteln. Für vertrauliche, große oder potenziell schädliche Anhänge zuerst einen geeigneten Übertragungsweg mit **security@nbb.de** abstimmen.

13. Koordinierte Offenlegung und Kommunikation

Veröffentlichungsstatus:

☐ Noch nicht veröffentlicht ☐ Veröffentlichung geplant

☐ Bereits veröffentlicht ☐ Unbekannt

Geplantes / tatsächliches Datum	
Fundstelle / Referenz	

Kontakt und Nennung:

☐ Für Rückfragen verfügbar ☐ Kontakt nur über Organisation

☐ Nennung als meldende Person erwünscht ☐ Keine öffentliche Nennung erwünscht

Vertraulichkeits- oder Kommunikationsanforderungen:

14. Erklärung und Datenschutz

Ich bestätige, dass die Angaben nach bestem Wissen vollständig und korrekt sind und ich zur Übermittlung der bereitgestellten Informationen und Anhänge berechtigt bin.

☐ Hinweis zum Umgang mit vertraulichen Informationen gelesen

☐ Firma NBB darf mich zur Bearbeitung kontaktieren

Ort, Datum	
Name	
Unterschrift	

Rücksendung:
Bitte senden Sie das ausgefüllte Formular an **security@nbb.de**.

Empfohlener Betreff:

Security Report - [Produkt] - [Kurzbeschreibung].

A. Nur zur internen Bearbeitung durch Firma NBB

Interner Bereich:
Nicht vom externen Melder auszufüllen. Dieser Bereich unterstützt Triage, Nachverfolgung und die dokumentierte Entscheidung über Melde- und Informationspflichten.

Incident-ID / Ticket	
Owner / Incident Manager	
Eingangskanal	
Zeitpunkt der Kenntniserlangung	
Betroffene Produktfamilie / Versionen	
Verknüpfte Tickets / CI-IDs	

Ersteinstufung:

☐ Schwachstelle
☐ Aktiv ausgenutzte Schwachstelle
☐ Sicherheitsvorfall
☐ Schwerwiegender Sicherheitsvorfall
☐ Kein Cybersecurity-Fall
☐ Bewertung offen

Begründung der Einstufung:

CRA-Meldepflicht geprüft durch / am	
24h-Zieltermin	
72h-Zieltermin	
Finaler Bericht / Zieltermin	
Meldestelle / Referenznummer	

Erforderliche interne Einbindung:

☐ Incident Response / PSIRT
☐ Produktentwicklung
☐ Systems Engineering
☐ Safety / Compliance
☐ Qualitätsmanagement
☐ Datenschutz
☐ Geschäftsleitung
☐ Kommunikation / Vertrieb
☐ Rechtliche Prüfung
☐ Externe Partner / Lieferanten

Sofortmaßnahmen / Eindämmung:

Korrekturmaßnahme und Kundenkommunikation:

Abschlussentscheidung / Lessons Learned: