

Vulnerability Disclosure Policy für Produkte mit digitalen Elementen der Novotechnik

1 Zweck und Geltungsbereich

Novotechnik Messwertaufnehmer OHG (kurz Novotechnik) betreibt einen koordinierten Prozess zur Annahme, Bewertung, Behandlung und verantwortungsvollen Offenlegung von Schwachstellen in Produkten mit digitalen Elementen, die von Novotechnik entwickelt, hergestellt oder unter eigenem Namen in Verkehr gebracht werden. Diese Richtlinie gilt derzeit für Produkte mit den Kundenschnittstellen CANopen, CAN J1939 und IO-Link. Ziel ist es, Risiken früh zu erkennen, Betroffene angemessen zu schützen und erforderliche Maßnahmen nachvollziehbar umzusetzen.

Diese Richtlinie regelt die Meldung und koordinierte Offenlegung von Produktschwachstellen gegen-über Novotechnik sowie die Information betroffener Nutzer. Gesetzliche Melde-, Informations- und Mitwirkungspflichten von Novotechnik gegenüber zuständigen Behörden oder Meldestellen bleiben hier-von unberührt und können unabhängig von der koordinierten öffentlichen Offenlegung erfüllt werden.

Allgemeine IT-Sicherheitsvorfälle, Datenschutzanfragen, physische Produktmängel und Supportanfragen ohne Cybersicherheitsbezug fallen nicht unter diese Richtlinie.

2 Erwartete Informationen für eine Meldung

Folgende Informationen sind für eine effiziente Bearbeitung und Bewertung der Schwachstelle im PSIRT notwendig:

- Produkt-/Typbezeichnung, Artikelnummer sowie Hardware- und Firmware-/Softwareversion
- Beschreibung des beobachteten Verhaltens, betroffene Schnittstelle und mögliche Sicherheitsauswirkungen in der Kundenapplikation
- Nachvollziehbare Schritte zur Reproduzierbarkeit, Betriebsumgebung, erforderliche Rechte oder physischer Zugriff
- Technische Informationen wie z. B. Protokolldateien (Logs), Bus-Traces oder Screenshots, soweit verfügbar
- Kontaktdaten für Rückfragen und Rückmeldungen, sofern gewünscht
- Bekannte CVE- oder CWE-Referenzen, soweit vorhanden
- Angaben zu einer geplanten oder bereits erfolgten Veröffentlichung der Schwachstelle

Die Angabe von Kontaktdaten ist freiwillig. Anonyme Meldungen werden so weit möglich ebenfalls geprüft. Ohne Kontaktmöglichkeit kann Novotechnik jedoch keine Rückfragen stellen oder über den Bearbeitungsstand informieren. Bei einer schwerwiegend eingestuften Meldung speichert Novotechnik die angegebenen Kontaktdaten, sofern vorhanden, in der internen Meldedatenbank. Die Pflege dieser Datenbank erfolgt auf der Grundlage der Bestimmungen der Datenschutz-Grundverordnung (DSGVO). Die Datenschutzerklärung der Novotechnik ist unter <https://www.novotechnik.de/datenschutz/> zu finden.

Für die Übermittlung vertraulicher technischer Informationen empfehlen wir die Verschlüsselung mittels des auf unserer PSIRT-Webseite veröffentlichten öffentlichen PGP-Schlüssels. Bitte übermitteln Sie Passwörter, private Schlüssel, produktive Zugangsdaten oder vertrauliche Kundendaten nicht unverschlüsselt.

3 Der PSIRT Schwachstellenmanagement-Prozess bei Novotechnik

Nr.	Schritt	Novotechnik-Aktivität
1	Eingang	Meldung dokumentieren, eine Referenznummer vergeben, den Schutzbedarf berücksichtigen und den Eingang innerhalb weniger Werktage bestätigen.
2	Validierung und Bewertung	Schwachstelle reproduzieren, Nachweise sichern, betroffene Produkte, Versionen und Komponenten identifizieren sowie eine Bewertung der gemeldeten Schwachstelle durchführen.
3	Behandlung und Verifikation	Koordination mit der Produktentwicklung zur Erarbeitung von Abhilfemaßnahmen. Gegebenenfalls werden Korrekturen bzw. Abhilfemaßnahmen geprüft, die Ihnen als Melder zur Überprüfung zur Verfügung gestellt werden können.
4	Offenlegung und Abschluss	Risikobasierte Kundeninformation oder Veröffentlichung eines Sicherheitshinweises nach Verifikation geeigneter Korrektur-, Abhilfe- oder Schutzmaßnahmen. Im Rahmen einer koordinierten Offenlegung kann der Melder auf Wunsch und nach vorheriger Abstimmung im Sicherheitshinweis genannt werden.

4 Risikobewertung und Abhilfe

Die Priorisierung erfolgt risikobasiert. Novotechnik berücksichtigt insbesondere den technischen Schweregrad, Angriffsvoraussetzungen, Hinweise auf eine aktive Ausnutzung, betroffene Produktstände sowie mögliche Auswirkungen auf Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität. Mögliche Safety- oder Anlagenfolgen werden berücksichtigt, soweit Novotechnik über die hierfür erforderlichen Informationen zur Kundenanwendung verfügt. Ein CVSS-Basiswert allein ist nicht ausschlaggebend für Art und Umfang der ergriffenen Maßnahmen.

5 Richtlinie zur Offenlegung von Schwachstellen

Nach Bereitstellung einer Abhilfemaßnahme veröffentlicht Novotechnik grundsätzlich einen Sicherheitshinweis zur behobenen Schwachstelle. Dieser enthält, soweit für die sichere Nutzung erforderlich und angemessen, Informationen zur Identifikation der betroffenen Produkte und Versionen, zu den möglichen Auswirkungen und zum Schweregrad sowie zu verfügbaren Sicherheitsupdates, Workarounds oder weiteren Schutzmaßnahmen.

Sofern die mit einer sofortigen Veröffentlichung verbundenen Risiken den Nutzen einer öffentlichen Offenlegung überwiegen, kann Novotechnik die öffentliche Bereitstellung einzelner Informationen angemessen verzögern, bis betroffene Nutzer Gelegenheit hatten, die vorgesehenen Abhilfemaßnahmen umzusetzen.

Novotechnik behandelt eingegangene Schwachstellenmeldungen und die Identität des Melders grundsätzlich vertraulich und gibt Informationen nur weiter, soweit dies zur Bearbeitung, Behebung, Koordination oder Erfüllung gesetzlicher Pflichten erforderlich ist.

Für weitere Fragen oder Rückmeldungen wenden Sie sich bitte per E-Mail an psirt@novotechnik.de