Meldung von Sicherheitslücken / Vulnerability Disclosure / Alphatech spol. s r. o.

Einführung

Die Sicherheit unserer Produkte hat für uns höchste Priorität. Wenn Sie eine Sicherheitslücke in einem Produkt oder Dienst von Alphatech entdeckt haben, bitten wir Sie, diese verantwortungsvoll über die unten angegebene Kontaktadresse zu melden. Ihre Meldung hilft uns, unsere Kunden zu schützen und die Sicherheit unserer Lösungen zu verbessern.

Kontakt

E-Mail: security@alphatech.cz

Empfohlene Inhalte der Meldung

Damit wir das Problem schnell überprüfen und beheben können, geben Sie bitte Folgendes an:

- Produktname / Modell und die betroffene Funktion (z. B. Web-UI, API, Update-Mechanismus)
- Firmware- / Softwareversion (ggf. Seriennummer oder andere Geräte-ID, falls verfügbar)
- Umgebung und Konfiguration (kurz: Netzwerktopologie, Betriebsmodus, offene Dienste/Ports)
- Beschreibung der Schwachstelle sowie erwartetes vs. tatsächliches Verhalten
- Schritte zur Reproduktion (idealerweise Schritt für Schritt)
- Nachweise / unterstützende Materialien (Logs, Screenshots, Wireshark-PCAP), sofern vorhanden
- Information, ob Hinweise auf eine aktive Ausnutzung vorliegen (IoCs, Zeitangaben, Quell-IP-Adressen usw.)

Unser weiteres Vorgehen

- Wir bestätigen den Eingang Ihrer Meldung so schnell wie möglich, in der Regel innerhalb von 24 Stunden.
- Die Meldung wird registriert und erhält eine eindeutige Kennung.
- Wir können Sie kontaktieren, um zusätzliche Informationen anzufordern oder Details zu verifizieren.
- Wenn eine schwerwiegende Schwachstelle bestätigt wird, bereiten wir geeignete Gegenmaßnahmen (Mitigation / Update) vor und veröffentlichen bei Bedarf eine Sicherheitsmitteilung (*Security Advisory*).

Koordinierte Offenlegung (Coordinated Disclosure)

Wir bitten um eine koordinierte Offenlegung. Bitte veröffentlichen Sie keine Details zur Schwachstelle, bevor eine Korrektur oder zumindest eine vorläufige Risikominderung verfügbar ist. Wenn Sie eine Veröffentlichung planen, kontaktieren Sie uns bitte im Voraus, damit wir das Vorgehen abstimmen können.

Sicherheitstests

Bitte führen Sie keine Tests durch, die:

- die Verfügbarkeit von Kundendiensten beeinträchtigen könnten,
- den Zugriff auf Daten Dritter ohne deren Zustimmung beinhalten,
- oder Geräte und Systeme betreffen, die Ihnen nicht gehören oder für die Sie keine Testberechtigung haben.

Rechtlicher Rahmen und Kommunikation

Im Falle von Sicherheitsvorfällen oder aktiv ausgenutzten Schwachstellen können wir gesetzlich verpflichtet sein, Meldungen an die zuständigen Behörden zu machen. Unsere Priorität ist es, Auswirkungen schnell zu begrenzen und betroffene Kunden mit praktischen Empfehlungen zu informieren.

Dank

Vielen Dank für Ihre verantwortungsvolle Meldung. Sicherheit ist Teamarbeit – und Ihr Beitrag hilft uns, unsere Kunden zu schützen.