

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 09.10.2026, 19:42 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	09.10.2026
Herausgeber	Maximilian Gilg, OT-Cyber.de, Rosenheim
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen
Online	https://ot-cyber.de/ot-lage/

Dieses Lagebild fasst öffentlich zugängliche Meldungen zusammen – automatisch zusammengestellt, ohne Gewähr. Die Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen in Deutschland, Österreich und der Schweiz.

Management Summary

Diese Ausgabe enthält 4 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

- Red Lion N-Tron 700: sieben Lücken in Industrial-Ethernet-Switches (ICSA-26-281-01, 08.10.)
- openPDC und openHistorian: Remote Code Execution und festes Admin-Passwort im Docker-Image (ICSA-26-281-02, 08.10.)

GESAMTBEWERTUNG

Hoch – vorrangig die Meldungen mit hoher Relevanz prüfen und umsetzen.

Lageübersicht

ID	Meldung	Relevanz
L-01	Red Lion N-Tron 700: sieben Lücken in Industrial-Ethernet-Switches (ICSA-26-281-01, 08.10.)	HOCH
L-02	openPDC und openHistorian: Remote Code Execution und festes Admin-Passwort im Docker-Image (ICSA-26-281-02, 08.10.)	HOCH
L-03	Satel Netco Design: vier Lücken, alle nur mit Konto ausnutzbar (ICSA-26-281-03, 08.10.)	MITTEL
L-04	Internationale Warnung vor China-nahen Angreifern rund um „Integrity Tech“, auch gegen Critical Manufacturing (AA26-281A, 08.10.)	MITTEL

Meldungen im Detail

L-01 Red Lion N-Tron 700: sieben Lücken in Industrial-Ethernet-Switches (ICSA-26-281-01, 08.10.)

Relevanz: HOCH

Betroffen sind Firmware bis 3.11.0 und Bootloader bis 2.0.6.1. Über SNMP sind Admin-Aktionen ohne Authentisierung möglich, etwa Konfiguration auslesen, Konten ändern oder Firmware tauschen (CVE-2026-33367, CVSS v4 9,3). Zugangsdaten liegen im Klartext in der Konfiguration und lassen sich per TFTP exportieren, den Export kann SNMP ohne Authentisierung anstoßen (CVE-2026-39460, CVSS v4 9,3). Ab Werk gesetzte Admin-Zugangsdaten bleiben aktiv (CVE-2026-32645, CVSS v4 9,2), Firmware-Updates verlangen keine Authentisierung (CVE-2026-29797), und ein bestimmter URL-Aufruf startet den Switch neu, was sich zu einer Reboot-Schleife (Denial of Service) skripten lässt (CVE-2026-39453). Eine Ausnutzung ist laut CISA nicht bekannt. Abhilfe: Firmware 3.11.1 oder neuer, bis dahin SNMP-Communities härten oder abschalten und den Web-Zugang sperren. Unsere Einschätzung: Diese Switches stecken oft im Kern von Anlagennetzen – Bestand im Asset-Inventar prüfen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-01>

Quelle: <https://www.assurantcyber.com/blog/icsa-26-281-01/>

Quelle: <https://www.strix.ai/cve/CVE-2026-33367>

L-02 openPDC und openHistorian: Remote Code Execution und festes Admin-Passwort im Docker-Image (ICSA-26-281-02, 08.10.)

Relevanz: **HOCH**

Sechs Lücken in der Software der Grid Protection Alliance, CISA nennt den Sektor Energie. Die kritischsten: Deserialisierung mit Remote Code Execution (CVE-2026-100730, CVSS 9,8), behoben in openPDC 2.9.482 und openHistorian 2.8.585, sowie ein festes Admin-Passwort im openPDC-Docker-Image (CVE-2026-105278, CVSS 9,8). Für das Docker-Image ist kein Fix geplant; der Hersteller rät ohnehin vom Produktivbetrieb der Docker-Images ab. Die Datenpublisher nehmen standardmäßig Verbindungen ohne Authentisierung an; der sichere Standard (nur loopback) gilt nur für Neuinstallationen – bestehende Installationen von Hand prüfen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-02>

Quelle: <https://securityonline.info/openpdc-openhistorian-vulnerabilities/>

Quelle: <https://www.strix.ai/cve/CVE-2026-100730>

L-03 Satel Netco Design: vier Lücken, alle nur mit Konto ausnutzbar (ICSA-26-281-03, 08.10.)

Relevanz: **MITTEL**

Betroffen sind alle Versionen vor 2.1.7. Die höchste Bewertung hat ein Path Traversal beim Datenexport (CVE-2026-101024, CVSS v3.1 8,8), dazu kommen Stored XSS (CVE-2026-105269, CVSS v4 8,5), ein weiteres Path Traversal und ein ReDoS. Für alle braucht der Angreifer mindestens Leserechte. Abhilfe: Update auf 2.1.7.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-03>

Quelle: <https://www.strix.ai/cve/CVE-2026-101024>

L-04 Internationale Warnung vor China-nahen Angreifern rund um „Integrity Tech“, auch gegen Critical Manufacturing (AA26-281A, 08.10.)

Relevanz: **MITTEL**

FBI, CISA, NSA und Partnerbehörden aus Großbritannien, Australien, Kanada, Japan, Neuseeland und Spanien beschreiben Akteure, deren Vorgehen Flax Typhoon ähnelt. Sie nutzen Password Spraying gegen Exchange und Microsoft 365, alte Lücken wie Pulse Connect Secure (CVE-2019-11510) und SoftEther-VPN-Clients für dauerhaften Fernzugriff, getarnt als „conhost.exe“ oder „dllhost.exe“. OT-Systeme nennt die Warnung nicht. Unsere Einschätzung: Threat Hunting nach SoftEther-Clients und unbekannten VPN-Tunneln auf Jump Hosts und in der DMZ, MFA für Remote Access durchsetzen (SANS CC4 – Secure Remote Access).

Quelle: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-281a>

Quelle: <https://www.picussecurity.com/resource/blog/cisa-aa26-281a-how-chinese-government-linked-actors-steal-sensitive-data>

Quelle: <https://www.ic3.gov/CSA/2026/261008.pdf>

Einordnung und Unterstützung: OT-Cyber.de · Am Esbaum 12, 83022 Rosenheim · +49 8031 8603164 · akademie@ot-cyber.de · <https://ot-cyber.de/>