OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 09.11.2026, 16:13 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	09.11.2026
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 2 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• **Node-RED-Lücke CVE-2026-58115 (u. a

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**Node-RED-Lücke CVE-2026-58115 (u. a	HOCH
L-02	**Update: Kühlanlagen: US-Behörden warnen gemeinsam vor Angriffen auf Kälte- und Kühlketten-Systeme (BleepingComputer, 05.11.2026)**: CISA, FBI, HHS, USDA und DOT haben dazu ein gemeinsames Advisory herausgegeben	MITTEL

Meldungen im Detail

L-01 **Node-RED-Lücke CVE-2026-58115 (u. a

Relevanz: HOCH

Siemens SIMATIC IoT2050 Advanced) wird ausgenutzt (CVSS 10, Warnung von VulnCheck vom 01.11.)**: Über die fehlende Authentifizierung an der Node-RED-HTTP-Schnittstelle können Angreifer ohne Anmeldung eigene Flows anlegen und damit Code mit höchsten Rechten ausführen. Betroffen sind IoT2050 Advanced mit Industrial OS und installiertem Node-RED. Laut VulnCheck lief der erste von VulnCheck beobachtete erfolgreiche Angriff am 30. Oktober, bis zum 1. November folgten 15 weitere von derselben IP-Adresse. Die Angreifer luden einen Linux-Bot nach, bei späteren Angriffen blieben Webshells zurück, über die sie weiter Befehle ausführen können. Siemens hat die Lücke am 11. August veröffentlicht, Version 4.3.4.1 und neuer enthalten den Fix. Gesucht wird gezielt nach Node-RED-Instanzen ohne adminAuth. Ob dabei IoT2050-Geräte getroffen wurden, nennt die Quelle nicht, die Angreifer suchen allgemein nach offenen Node-RED-Instanzen. Laut Quelle steckt Node-RED auch in kommerziellen ICS/OT-Geräten. IoT2050-Betreiber in DACH sollten auf 4.3.4.1 oder neuer aktualisieren. Generell gilt: Node-RED nicht aus dem Internet erreichbar lassen, adminAuth einschalten und nach unbekannten Flows suchen.

Quelle: https://www.securityweek.com/critical-node-red-flaw-exploited-in-attacks/

L-02 **Update: Kühlanlagen: US-Behörden warnen gemeinsam vor Angriffen auf Kälte- und Kühlketten-Systeme (BleepingComputer, 05.11.2026)**: CISA, FBI, HHS, USDA und DOT haben dazu ein gemeinsames Advisory herausgegeben

Relevanz: MITTEL

Darin warnen sie vor weltweiten Angriffen auf industrielle Kühl- und Kühlketten-Überwachung, die unter anderem Brandgefahr verursachen können. Hersteller nennt der Bericht nicht.

Quelle:
https://bleepingcomputer.com/news/security/fbi-cisa-warn-of-cyberattacks-targeting-refrigeration-systems

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