OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 16.11.2026, 07:24 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	16.11.2026
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 0 mit hoher Relevanz für Betreiber in DACH.

GESAMTBEWERTUNG

Mittel – keine akute Lage, Meldungen im regulären Schwachstellen-Management bearbeiten.

Lageübersicht

ID	Meldung	Relevanz
L-01	**N-able N-central: Exploit-Kette „4EverAble2Shell“ wird aktiv ausgenutzt**: Laut The Hacker News vom 13.11. kombinieren Angreifer die kritische Apache-Axis-Lücke CVE-2026-90436 (CVSS 9,8) mit einer Rechteausweitung in N-central und erhalten so Root-Zugriff auf den Server	MITTEL
L-02	**Siemens ProductCERT veröffentlicht Advisory-Policy**: Siemens ProductCERT hat eine Policy für seine Security Advisories veröffentlicht, laut Versionshistorie als Erstfassung mit Datum 12.11.2026	NIEDRIG

Meldungen im Detail

L-01 **N-able N-central: Exploit-Kette „4EverAble2Shell“ wird aktiv ausgenutzt**: Laut The Hacker News vom 13.11. kombinieren Angreifer die kritische Apache-Axis-Lücke CVE-2026-90436 (CVSS 9,8) mit einer Rechteausweitung in N-central und erhalten so Root-Zugriff auf den Server

Relevanz: MITTEL

Über N-central verwalten IT-Dienstleister die Rechner und Server ihrer Kunden. Laut Huntback haben die Angreifer auf 21 N-central-Servern einen Kryptominer (XMRig) installiert, 19 davon liefen schon mit Hotfix 2. Hotfix 2 allein reicht also nicht. N-able rät, Agents und Probes zu aktualisieren und den Zugang über die Legacy API abzuschalten. Unsere Einschätzung: Das kann Stadtwerke, Zweckverbände und Maschinenbauer betreffen, deren Systemhaus N-central für die Fernwartung nutzt. Fragen Sie Ihren Dienstleister, ob er N-central einsetzt, ob Agents und Probes aktualisiert sind und ob die Legacy API aus ist (CC4 Secure Remote Access der SANS Five ICS Critical Controls).

Quelle: https://thehackernews.com/2026/11/hackers-exploit-n-central-flaws-to.html

L-02 **Siemens ProductCERT veröffentlicht Advisory-Policy**: Siemens ProductCERT hat eine Policy für seine Security Advisories veröffentlicht, laut Versionshistorie als Erstfassung mit Datum 12.11.2026

Relevanz: NIEDRIG

Advisories gibt es demnach als HTML und maschinenlesbar im CSAF-Format, verteilt über einen ROLIE-Feed. In Arbeit sind laut Siemens unter anderem eine API für automatische Abfragen von Produkt- und Schwachstellendaten sowie mehr Angaben zu Schwachstellen in Fremdkomponenten. Unsere Einschätzung: Wer Siemens-Leittechnik betreibt, kann die CSAF-Daten automatisch mit dem eigenen Asset-Inventar abgleichen und sieht schneller, welche Advisories die eigene Anlage betreffen (CC5 Risk-Based Vulnerability Management).

Quelle: https://productcert.siemens.com/advisory-policy/

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