OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 12.11.2026, 07:31 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	12.11.2026
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 1 Meldung, 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	UPDATE: **PHP2Shell erreicht Weidmüller-Security-Router: auf IE-SR-4TX und IE-SR-4GT fällt nur die Weboberfläche aus (CERT@VDE VDE-2026-152, CVE-2026-109618, 10.11.)**: Nach Helmholz (Fernwartungsportal myREX24) meldet mit Weidmüller ein weiterer OT-Hersteller eine der PHP2Shell-Lücken in seiner Firmware	MITTEL

Meldungen im Detail

L-01 UPDATE: **PHP2Shell erreicht Weidmüller-Security-Router: auf IE-SR-4TX und IE-SR-4GT fällt nur die Weboberfläche aus (CERT@VDE VDE-2026-152, CVE-2026-109618, 10.11.)**: Nach Helmholz (Fernwartungsportal myREX24) meldet mit Weidmüller ein weiterer OT-Hersteller eine der PHP2Shell-Lücken in seiner Firmware

Relevanz: MITTEL

Laut Weidmüller enthält die Firmware der Security-Router IE-SR-4TX und IE-SR-4GT vor Version 2.3.4 eine PHP-Version, die von CVE-2026-109618 betroffen ist, einer der beiden PHP2Shell-Lücken in PHP. Betroffen sind acht Varianten, darunter die LTE/4G-Modelle und die M-Varianten. Auf den Routern ist nach Angabe des Herstellers nur die Weboberfläche betroffen: Sie ist nicht erreichbar, bis der PHP-Worker neu gestartet ist. Vertraulichkeit und Integrität sind nicht betroffen, Routing und Firewall laufen weiter. Deshalb bewertet Weidmüller die Lücke für diese Geräte mit CVSS 3.1: 5,3, für PHP allgemein stehen 9,8. Der Fix ist Firmware 2.3.4 oder neuer. Unsere Einordnung: Da Routing und Firewall laut Hersteller weiterlaufen, ist das kein akuter Notfall. Ein Ausfall der Weboberfläche am Edge-Gerät ist aber ein Anlass, den Firmware-Stand der Router im Asset-Inventar zu kennen und das Update einzuplanen. Das ist ein Fall für CC5 Risk-Based Vulnerability Management der SANS Five ICS Critical Controls.

Quelle: https://certvde.com/en/advisories/VDE-2026-152/

Quelle: https://ot-cyber.de/ot-lage/2026-10-27.html

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