OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 17.11.2026, 16:07 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	17.11.2026
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 5 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

• **CODESYS Automation Server Connector und Service Tool: zwei Lücken, eine davon kann zu Code-Ausführung führen**: Laut CERT@VDE (VDE-2026-145) sind der Automation Server Connector und das CODESYS Service Tool in allen Versionen vor 1.40 betroffen, das Update auf Version 1.40 schließt beide Lücken

• **Update Kühlanlagen: Angreifer tasten neue Lücken in Copeland XWEB EVO ab**: VulnCheck hat 14 Schwachstellen in den Kühlstellen-Steuerungen Copeland XWEB EVO (früher Dixell) veröffentlicht

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**CODESYS Automation Server Connector und Service Tool: zwei Lücken, eine davon kann zu Code-Ausführung führen**: Laut CERT@VDE (VDE-2026-145) sind der Automation Server Connector und das CODESYS Service Tool in allen Versionen vor 1.40 betroffen, das Update auf Version 1.40 schließt beide Lücken	HOCH
L-02	**Dragos Q3 2026: 1.266 Ransomware-Vorfälle in der Industrie, 11 % mehr als im Vorquartal**: Dragos zählt im dritten Quartal 1.266 Ransomware-Vorfälle bei Industrieunternehmen weltweit, nach 1.140 im zweiten Quartal	MITTEL
L-03	**Update Kühlanlagen: Angreifer tasten neue Lücken in Copeland XWEB EVO ab**: VulnCheck hat 14 Schwachstellen in den Kühlstellen-Steuerungen Copeland XWEB EVO (früher Dixell) veröffentlicht	HOCH
L-04	**NoisyTCP: Lücke im Linux-Kernel lässt Systeme aus der Ferne abstürzen (CVE-2026-99288)**: Laut BleepingComputer vom 16.11. steckt der Fehler im TCP-Code des Linux-Kernels	MITTEL
L-05	**Google Project Zero gibt Herstellern weniger Zeit bis zur Veröffentlichung**: Laut Help Net Security vom 16.11. will Project Zero gemeldete Lücken 90 Tage nach der Meldung an den Hersteller veröffentlichen, auch wenn es noch keinen Fix gibt	MITTEL

Meldungen im Detail

L-01 **CODESYS Automation Server Connector und Service Tool: zwei Lücken, eine davon kann zu Code-Ausführung führen**: Laut CERT@VDE (VDE-2026-145) sind der Automation Server Connector und das CODESYS Service Tool in allen Versionen vor 1.40 betroffen, das Update auf Version 1.40 schließt beide Lücken

Relevanz: HOCH

Bei CVE-2026-118496 (CVSS 7,5) verarbeiten die Produkte eine vom Server gelieferte URL ohne ausreichende Prüfung. Wer einen bösartigen Automation Server betreibt oder sich als Man-in-the-Middle dazwischenschaltet, kann laut Advisory damit Code mit den Rechten des Benutzers ausführen, der das betroffene Produkt nutzt. Bei CVE-2026-118497 (CVSS 6,8) prüfen die Produkte das TLS-Zertifikat des Automation Servers bei der Registrierung nicht ausreichend. Ob die Lücken schon ausgenutzt werden, sagt das Advisory nicht. Unsere Einschätzung: Betroffen sind Engineering- und Konfigurationswerkzeuge, nicht die CODESYS-Runtime in den Steuerungen. Wer die Fernverwaltung über den Automation Server nutzt, sollte Connector und Service Tool auf den Engineering-Rechnern zeitnah aktualisieren (Unsere Einordnung: CC4 Secure Remote Access).

Quelle: https://certvde.com/en/advisories/VDE-2026-145/

L-02 **Dragos Q3 2026: 1.266 Ransomware-Vorfälle in der Industrie, 11 % mehr als im Vorquartal**: Dragos zählt im dritten Quartal 1.266 Ransomware-Vorfälle bei Industrieunternehmen weltweit, nach 1.140 im zweiten Quartal

Relevanz: MITTEL

Die Fertigung ist mit 876 Vorfällen (69 %) am stärksten betroffen. Die Gruppen Qilin und The Gentlemen kommen zusammen auf 362 Vorfälle (29 %), The Gentlemen allein auf 167. INC Ransom liegt mit 58 Opfern aus der Industrie auf Platz drei. Unsere Einschätzung: Für Maschinenbauer und Zulieferer in DACH heißt das, Wiederanlauf ohne IT-Netz zu planen und zu üben, damit die Produktion nach einem Angriff nicht tagelang steht (Unsere Einordnung: CC1 ICS Incident Response).

Quelle: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2026

L-03 **Update Kühlanlagen: Angreifer tasten neue Lücken in Copeland XWEB EVO ab**: VulnCheck hat 14 Schwachstellen in den Kühlstellen-Steuerungen Copeland XWEB EVO (früher Dixell) veröffentlicht

Relevanz: HOCH

Laut SecurityWeek vom 16.11. wurden die CVE-Einträge am 12.11. veröffentlicht, und die Sensoren von VulnCheck sahen die ersten Ausnutzungsversuche schon innerhalb von zwei Stunden. Sie zielten auf CVE-2026-124014, mit der Angreifer ohne Anmeldung die Systemkonfiguration überschreiben können. Am 13.11. folgten laut SecurityWeek Versuche gegen CVE-2026-124010, eine Befehlsausführung als root ohne Login. Fünf der Lücken werden nicht mehr behoben, denn Copeland hat den Software-Support für XWEB EVO am 16.03.2026 beendet und rät zum Umstieg auf XWEB Pro. Laut Onyphe-Daten, die VulnCheck zitiert, sind fast 2000 XWEB-EVO-Geräte aus dem Internet erreichbar. VulnCheck sieht in den Scans keinen Beleg für die Sabotage an französischen Supermärkten im Oktober, die Frankreich dem Iran zuschreibt. Unsere Einschätzung: Betroffen sein können Kühlhäuser, Lebensmittel-Produktionsstätten, Metzgereien und Großküchen von Kliniken oder Kommunen in Bayern, Salzburg und Tirol, die ältere Dixell- oder Copeland-Steuerungen über Fernwartung erreichen. Diese Geräte gehören sofort aus dem Internet, Zugriff nur noch über VPN, und der Umstieg auf eine unterstützte Plattform sollte jetzt geplant werden (CC4 Secure Remote Access der SANS Five ICS Critical Controls).

Quelle:
https://www.securityweek.com/hackers-probe-newly-disclosed-flaws-in-copeland-refrigeration-controllers/

L-04 **NoisyTCP: Lücke im Linux-Kernel lässt Systeme aus der Ferne abstürzen (CVE-2026-99288)**: Laut BleepingComputer vom 16.11. steckt der Fehler im TCP-Code des Linux-Kernels

Relevanz: MITTEL

Angreifer brauchen keinen Login: Präparierte TCP-Pakete bringen Kernel und Betriebssystem zum Absturz. Daten ändern oder Code ausführen können sie damit laut Quelle nicht. Ein Patch ist verfügbar und schon im Mainline-Kernel. Wer nicht sofort patchen kann, kann laut dem Entdecker SYN-Cookies abschalten, verliert dann aber Schutz gegen SYN-Floods. Ein OT-Bezug steht nicht in der Quelle. Unsere Einschätzung: Viele Router, Edge-Geräte, HMI-Panels und Fernwirk-Gateways bei Stadtwerken laufen auf Linux, und Kernel-Patches kommen dort oft erst spät als Firmware an. Fragen Sie bei den Herstellern nach, wann ein Update kommt (CC5 Risk-Based Vulnerability Management).

Quelle:
https://www.bleepingcomputer.com/news/linux/new-noisytcp-linux-kernel-flaw-lets-attackers-crash-servers/

L-05 **Google Project Zero gibt Herstellern weniger Zeit bis zur Veröffentlichung**: Laut Help Net Security vom 16.11. will Project Zero gemeldete Lücken 90 Tage nach der Meldung an den Hersteller veröffentlichen, auch wenn es noch keinen Fix gibt

Relevanz: MITTEL

Damit endet die bisherige Regel „90 + 30“, bei der Hersteller nach dem Fix noch 30 Tage zum Ausrollen bekamen. Am 02.02.2027 sinkt die Frist auf 60 Tage, am 03.01.2028 auf 30 Tage, und auch dann gibt es keinen Extra-Monat für das Ausrollen. Unsere Einschätzung: Wer bei Firmware lange Freigabezyklen hat (Leittechnik, Wasser, Netze), wird öfter Lücken kennen, für die noch kein Patch eingespielt ist. Segmentierung und Notfallmaßnahmen ohne Patch werden damit wichtiger (CC2 Defensible Architecture).

Quelle: https://www.helpnetsecurity.com/2026/11/16/google-project-zero-disclosure-policy/

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