OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 45/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
Berichtszeitraum	30.10.2026–06.11.2026
Version	1.0
Datum	06.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 45 wurde eine Gateway-Lücke ausgenutzt, wie sie in vielen Maschinen steckt. Laut VulnCheck greifen Angreifer Siemens SIMATIC IoT2050 mit Node-RED über CVE-2026-58115 (CVSS 10) an, der erste Angriff wurde am 30.10. beobachtet. Dazu kommt ein Siemens Advisory zu Industrial Edge: Für mehrere Management-Apps gibt es noch keinen Fix, Siemens empfiehlt nur Mitigationen. Bei der Kühlanlagen-Welle in Supermärkten zeigt sich in Deutschland erstmals der Angriffsweg. Laut dpa wurde in Wetter-Volmarstein nicht der Markt angegriffen, sondern die Firma, die die Anlagen per Fernwartung betreut. Das betrifft jeden Hersteller und Integrator, der Fernzugänge zu Kundenanlagen betreibt.

CERT@VDE hat in dieser Woche mehrere Advisories zu DACH-Herstellern veröffentlicht. Bei WAGO können Angreifer über das PHP im integrierten Webserver von Steuerungen ohne Anmeldung Code ausführen (CVSS 9,8). Bei Phoenix Contact PLCnext Engineer werden GSDX-Signaturen nicht geprüft und Plug-ins lassen sich manipulieren. Mehrere Phoenix-Tools enthalten eine verwundbare CodeMeter Runtime. Welotec hat Lücken in TK-Routern gemeldet (VDE-2026-119, Ausnutzung nur mit hohen Rechten), die häufig für die Fernwartung genutzt werden. Für Komponentenhersteller ist das ein Probelauf für den CRA: Seit dem 11.09.2026 müssen sie aktiv ausgenutzte Schwachstellen über die ENISA-Plattform melden.

GESAMTBEWERTUNG

Lage erhöht: In einem verbreiteten Industrie-Gateway wird eine Lücke aktiv ausgenutzt, und über einen Fernwartungsdienstleister gab es einen Angriff mit physischen Folgen. Vorrang haben das Inventar und die Härtung von Node-RED/IoT2050, Industrial Edge und den eigenen Fernwartungszugängen.

Trends

• Angreifer zielen gezielt auf Edge-Geräte und Gateways in Maschinen (IoT2050/Node-RED, Industrial Edge, Router), weil diese oft offen und lange ungepatcht im Feld stehen.

• Fernwartungsdienstleister werden zum Sammelzugang: Ein kompromittierter Service öffnet viele Kundenanlagen auf einmal, wie bei den Kühlanlagen.

• Lücken in Fremdkomponenten (PHP, Brotli, CodeMeter, CODESYS) kommen bei vielen Herstellern gleichzeitig an, ohne SBOM fehlt der Überblick.

• Engineering-Werkzeuge und Gerätebeschreibungen (GSDX, Plug-ins) werden zur Lieferkette in die Steuerung.

• Seit dem 11.09.2026 gilt die CRA-Meldepflicht für aktiv ausgenutzte Schwachstellen, Fälle wie IoT2050 sind für Hersteller die Probe dafür.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Kühlanlagen-Angriffe in Deutschland: Weg führte offenbar über den Fernwartungsdienstleister	HOCH	Handelsblatt (dpa), 03.11.

ID	Meldung	Relevanz	Quelle
L-02	Siemens Industrial Edge: Brotli-Lücke CVE-2026-111497 (CVSS 9,8), für sieben Management-Apps noch kein Fix (SSA-443410)	HOCH	Siemens ProductCERT, 30.10.
L-03	WAGO-Steuerungen: PHP2Shell, Codeausführung ohne Anmeldung über den Webserver (CVE-2026-109618, CVSS 9,8)	HOCH	CERT@VDE (VDE-2026-132), 02.11.
L-04	Phoenix Contact PLCnext Engineer: GSDX-Signaturen werden nicht geprüft, Plug-in-Validierung umgehbar (VDE-2026-121)	MITTEL	CERT@VDE (VDE-2026-121), 04.11.
L-05	Phoenix Contact: CodeMeter-Runtime-Lücken in Software-Tools (VDE-2026-098, bis CVSS 8,6)	MITTEL	CERT@VDE (VDE-2026-098), 04.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 06.11.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt. Siemens S7 = Port 102 (alle ISO-TSAP-Dienste, nicht nur echte S7-Steuerungen), OPC UA = Standardport 4840.

Region	Gesamt	Top-Protokolle
Deutschland	143185	DNP3: 32440, OMRON FINS: 26119, ProConOS: 16052, Siemens S7: 7764, OPC UA: 5141
Österreich	4790	HMI/VNC: 1046, DNP3: 970, Niagara Fox: 472, Siemens S7: 387, OPC UA: 158

Meldungen im Detail

L-01 Kühlanlagen-Angriffe in Deutschland: Weg führte offenbar über den Fernwartungsdienstleister

HOCH Handelsblatt (dpa), 03.11.

Was ist neu: Laut dpa sind neben Lilienthal auch Märkte in Wuppertal, Wetter bei Hagen, Niederbayern, dem Münsterland und der Westpfalz betroffen. Der Markt in Wetter-Volmarstein gibt an, der Angriff sei auf die Firma erfolgt, die die Kühlanlagen aus der Ferne wartet. Wer dahintersteckt, ist unklar.

Bedeutung: Hier wurde ein Dienstleister mit Fernzugang zu vielen Kundenanlagen zum Einfallstor. Dieselbe Rolle haben Maschinenbauer und Systemintegratoren mit eigenen Serviceportalen. Wird so ein zentraler Zugang kompromittiert, trifft es alle Kunden zugleich.

Empfehlung: Fernwartung über ein zentrales Gateway mit MFA, Freigabe je Sitzung durch den Kunden und Protokollierung betreiben. Gemeinsam genutzte Service-Zugangsdaten über mehrere Kunden hinweg abschaffen.

Quelle: https://www.handelsblatt.com/politik/deutschland/hacker-attacke-cyberangriffe-auch-auf-kuehlanlagen-deutscher-supermaerkte/100266999.html ✓ geprüft

L-02 Siemens Industrial Edge: Brotli-Lücke CVE-2026-111497 (CVSS 9,8), für sieben Management-Apps noch kein Fix (SSA-443410)

HOCH Siemens ProductCERT, 30.10.

Was ist neu: Siemens prüft die Auswirkung der Brotli-Lücke CVE-2026-111497 auf Industrial Edge. Hub und Management Cloud sind laut Advisory zentral behoben. Für Apps wie Edge OPC UA Server Configurator, Databus Configurator oder Flow Creator Configurator gibt es noch keinen Fix.

Bedeutung: Wer Industrial Edge in Maschinen oder Linien integriert, muss die Mitigationen beim Kunden umsetzen oder anstoßen. Ohne installierte Management-Apps ist laut Siemens nichts zu tun.

Empfehlung: Je IEM-Instanz prüfen, welche Management-Apps installiert sind. Die betroffenen Apps nach Siemens-Vorgabe entfernen und das IEM vom übrigen Netz trennen, bis Fixes da sind.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-443410.html ✓ geprüft

L-03 WAGO-Steuerungen: PHP2Shell, Codeausführung ohne Anmeldung über den Webserver (CVE-2026-109618, CVSS 9,8)

HOCH CERT@VDE (VDE-2026-132), 02.11.

Was ist neu: Zwei Use-after-free-Lücken in der PHP-Laufzeit (CVE-2026-109618 mit CVSS 9,8, CVE-2026-109619 mit CVSS 8,1) erlauben Codeausführung aus der Ferne. Betroffen ist wago_os_linux unter 4.10.4 (FW32), wenn der integrierte Webserver aktiv ist. Hinweise auf Ausnutzung gibt es im Advisory nicht.

Bedeutung: WAGO-PFC-Steuerungen stecken in vielen Maschinen aus DACH, oft mit aktivem Web-Based Management. Als Hersteller müssen Sie den Kunden das Update liefern oder freigeben, mit Blick auf den CRA am besten dokumentiert.

Empfehlung: Auslieferungsstände abgleichen, FW32 4.10.4 testen und freigeben, sobald WAGO sie bereitstellt (für FW31 gibt es einen IPK-Patch). Bis dahin den Webserver über die Sicherheitseinstellungen abschalten, wie WAGO es empfiehlt.

Quelle: https://certvde.com/en/advisories/VDE-2026-132/ ✓ geprüft

L-04 Phoenix Contact PLCnext Engineer: GSDX-Signaturen werden nicht geprüft, Plug-in-Validierung umgehbar (VDE-2026-121)

MITTEL CERT@VDE (VDE-2026-121), 04.11.

Was ist neu: Betroffen sind alle Versionen von PLCnext Engineer vor 2026.6, mit drei CVEs (CVE-2026-110935 und CVE-2026-110022 mit CVSS 8,4, CVE-2026-110021 mit CVSS 6,2). Manipulierte GSDML-Gerätebeschreibungen können als gültig erscheinen, und präparierte Plug-ins können Code im Kontext des Nutzers ausführen.

Bedeutung: Gerätebeschreibungen und Plug-ins sind eine Lieferkette direkt in die Steuerung. Eine gefälschte GSDX-Datei kann in Projekte und auf PROFINET-Controller gelangen, ohne dass die Signaturprüfung anschlägt.

Empfehlung: Engineering-Arbeitsplätze auf 2026.6 bringen und Plug-ins sowie GSD-Dateien nur aus geprüften Herstellerquellen beziehen. Bis zum Update GSDX-Signaturen mit externen Werkzeugen prüfen, wie Phoenix Contact rät.

Quelle: https://certvde.com/en/advisories/VDE-2026-121/ ✓ geprüft

L-05 Phoenix Contact: CodeMeter-Runtime-Lücken in Software-Tools (VDE-2026-098, bis CVSS 8,6)

MITTEL CERT@VDE (VDE-2026-098), 04.11.

Was ist neu: Fünf CVEs in der CodeMeter Runtime betreffen Tools wie Activation Wizard, PLCnext Engineer, IO-Link ENGINEER und MTP DESIGNER. Im Servermodus können Angreifer aus der Ferne Konfigurationsdaten lesen und Server.ini überschreiben (CVE-2026-81573, CVSS 8,6). Phoenix-Contact-Fixes sollen im Q4 2026 folgen.

Bedeutung: CodeMeter von WIBU-SYSTEMS wird auch von vielen anderen Herstellern zur Lizenzierung eingesetzt und läuft auf Service-Laptops, die in Kundennetze gehen. Eigene Produkte mit CodeMeter gehören deshalb ins SBOM-Review.

Empfehlung: CodeMeter Runtime direkt von WIBU-SYSTEMS aktualisieren und den Netzwerkserver abschalten, wo er nicht gebraucht wird (ab 9.00: cmu --disable-network-server). Eigene SBOMs auf CodeMeter prüfen.

Quelle: https://certvde.com/en/advisories/VDE-2026-098/ ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Fernwartungsplattform härten: MFA, Kundenfreigabe je Sitzung, eigene Zugangsdaten je Kunde, Protokolle auswerten [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Industrial-Edge-Instanzen nach SSA-443410 absichern und das IEM vom übrigen Netz trennen [CC2 Defensible Architecture]	L-02	HOCH	sofort
M-03	Freigabeprozess für Firmware-Updates (WAGO FW32, Welotec, PLCnext) mit SBOM-Abgleich und Kundeninformation aufbauen [CC5 Risk-Based Vulnerability Management]	L-03	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Wissen wir, bei welchen Kunden IoT2050 mit Node-RED, WAGO-PFC oder Welotec-Router aus unseren Lieferungen laufen, und in welchem Firmware-Stand?

2. Wer entscheidet bei uns innerhalb von 24 Stunden, ob eine aktiv ausgenutzte Lücke in unserem Produkt nach CRA an die ENISA-Plattform gemeldet wird?

3. Läuft unsere Fernwartung mit MFA, Freigabe durch den Kunden je Sitzung und getrennten Zugangsdaten je Kunde?

4. Stehen CodeMeter, PHP und Brotli in unseren SBOMs, und wer prüft neue Advisories dagegen?

5. Woher beziehen unsere Engineers GSD-Dateien und Plug-ins, und wird die Herkunft geprüft?

Maßnahmen dieser Woche

1. Installierte Basis an IoT2050 Advanced mit Node-RED ermitteln, Kunden zum Update auf V4.3.4-1 anschreiben und erreichbare Geräte auf fremde Flows prüfen.

2. In Industrial-Edge-Projekten die betroffenen Management-Apps nach SSA-443410 entfernen (fünf) bzw. stoppen (zwei) und das IEM per Firewall abschirmen.

3. WAGO-Steuerungen in Kundenprojekten auf FW32 4.10.4 planen, bis dahin den Webserver abschalten, wo er nicht gebraucht wird.

4. Fernwartungsportal prüfen: MFA, Sitzungsfreigabe, Protokolle der letzten 30 Tage, gemeinsam genutzte Service-Passwörter entfernen.

5. PLCnext Engineer auf 2026.6 und CodeMeter Runtime auf V8.41a/V9.10 aktualisieren, Netzwerkserver von CodeMeter abschalten.

6. Ablauf für die CRA-Meldung (Frühwarnung innerhalb von 24 Stunden) an einem Fall wie IoT2050 durchspielen.

HINWEIS ZUR QUELLENLAGE

Advisories und Daten habe ich direkt bei CERT@VDE, Siemens ProductCERT und CISA nachgelesen, die IoT2050-Ausnutzung bei SecurityWeek (Ursprung VulnCheck, Honeypot-Daten, Zahl echter Opfer unklar). Die Kühlanlagen-Angriffe kennt nur die Presse (dpa). Den Hersteller Danfoss nennt Handelsblatt nicht, eine Behördenmeldung zu Deutschland habe ich nicht gefunden. Nicht aufgenommen: TeamViewer TV-2026-1011 (vom 27.10., also vor dem Berichtszeitraum), WAGO VDE-2025-081 zu CODESYS (06.11., Erstausgabe laut Revisionshistorie am 21.09.) und Festo Didactic VDE-2026-139 (02.11., PHP2Shell in FactoryViews und MES4). Neue Fakten zu harmonisierten Normen für CRA oder Maschinenverordnung im Amtsblatt habe ich für diese Woche nicht gefunden. Die Maschinenverordnung gilt ab dem 20.01.2027. Alle Quellenlinks wurden am 06.11.2026 automatisch aufgerufen und inhaltlich geprüft. 2 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.