OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 11.11.2026, 16:11 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	11.11.2026
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 6 Meldungen, davon 3 mit hoher Relevanz für Betreiber in DACH.

• **Siemens SIMATIC WinCC Graphics Designer: präparierte Datei kann beim Öffnen Code ausführen, noch kein Fix (SSA-979641, CVE-2026-59082, 10.11.)**: Laut Siemens enthält der Graphics Designer von WinCC vor V8.2 eine Lücke, über die beim Öffnen einer Datei aktive Inhalte ausgeführt werden

• **Helmholz myREX24V2 und myREX24V2.virtual: zwölf Lücken, darunter XSS mit CVSS 9,3 (CERT@VDE VDE-2026-141, 10.11.)**: Laut CERT@VDE könnten die Lücken Remote Code Execution, DoS oder das Abfließen von Informationen erlauben

• □ UPDATE: **Helmholz myREX24V2 und myREX24V2.virtual: php2shell, Fix erst mit 2.21.6 (CERT@VDE VDE-2026-160, 10.11.)**: Betroffen ist die Firmware vor 2.21.6

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**Siemens SIMATIC WinCC Graphics Designer: präparierte Datei kann beim Öffnen Code ausführen, noch kein Fix (SSA-979641, CVE-2026-59082, 10.11.)**: Laut Siemens enthält der Graphics Designer von WinCC vor V8.2 eine Lücke, über die beim Öffnen einer Datei aktive Inhalte ausgeführt werden	HOCH
L-02	**Siemens meta-iot2050: Command Injection im Firmware-Update-Tool, Fix noch nicht veröffentlicht (SSA-724261, CVE-2026-109830, 10.11.)**: Betroffen sind alle Versionen von meta-iot2050 ab V01.03.01	MITTEL
L-03	**Beckhoff: drei Lücken im Treiber TcRouter.sys geben lokalen Nutzern volle Systemrechte (CERT@VDE VDE-2026-087, 11.11.)**: Über offene IOCTL-Aufrufe im Treiber können lokale Nutzer oder Prozesse mit geringen Rechten auf physischen Speicher zugreifen und das Gerät vollständig übernehmen (CVE-2026-18767, CVE-2026-18768 und CVE-2026-18769, je CVSS 3.1: 7,8)	MITTEL
L-04	**SANS 2026 State of ICS/OT Security Survey: 34 % der Befragten meldeten einen Vorfall (Pressemitteilung vom 10.11.)**: Im Vorjahr waren es 22 %, laut SANS der größte Anstieg innerhalb eines Jahres in der Geschichte der Umfrage. 72 % dieser Vorfälle haben den Betrieb gestört	MITTEL
L-05	**Helmholz myREX24V2 und myREX24V2.virtual: zwölf Lücken, darunter XSS mit CVSS 9,3 (CERT@VDE VDE-2026-141, 10.11.)**: Laut CERT@VDE könnten die Lücken Remote Code Execution, DoS oder das Abfließen von Informationen erlauben	HOCH
L-06	□ UPDATE: **Helmholz myREX24V2 und myREX24V2.virtual: php2shell, Fix erst mit 2.21.6 (CERT@VDE VDE-2026-160, 10.11.)**: Betroffen ist die Firmware vor 2.21.6	HOCH

Meldungen im Detail

L-01 **Siemens SIMATIC WinCC Graphics Designer: präparierte Datei kann beim Öffnen Code ausführen, noch kein Fix (SSA-979641, CVE-2026-59082, 10.11.)**: Laut Siemens enthält der Graphics Designer von WinCC vor V8.2 eine Lücke, über die beim Öffnen einer Datei aktive Inhalte ausgeführt werden

Relevanz: HOCH

Ein Angreifer könnte so beliebigen Code auf dem Rechner ausführen (CVSS 3.1: 7,8, CVSS 4.0: 8,5). Einen Fix gibt es noch nicht, Siemens bereitet ihn vor und empfiehlt, nur Dateien aus vertrauenswürdigen Quellen zu öffnen. Zu einer Ausnutzung sagt das Advisory nichts. In der Praxis heißt das: Projektdateien von Integratoren, aus Mails oder vom USB-Stick nicht direkt auf dem Engineering- oder Leitstellenrechner öffnen, sondern vorher prüfen und auf einem getrennten System ansehen. Unsere Einordnung: Das ist ein Fall für CC2 Defensible Architecture der SANS Five ICS Critical Controls.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-979641.html

L-02 **Siemens meta-iot2050: Command Injection im Firmware-Update-Tool, Fix noch nicht veröffentlicht (SSA-724261, CVE-2026-109830, 10.11.)**: Betroffen sind alle Versionen von meta-iot2050 ab V01.03.01

Relevanz: MITTEL

Das Update-Tool übernimmt Teile einer Konfigurationsdatei und führt sie ungeprüft aus. Wer diese Datei verändern kann, könnte so Befehle mit Root-Rechten ausführen lassen (CVSS 3.1: 7,3, lokal, mit Benutzerinteraktion). Laut Siemens ist der Fix schon im Master-Branch und kommt mit dem nächsten Release. Bis zum Release sollten Betreiber prüfen, wer auf den betroffenen Systemen Konfigurationsdateien ablegen oder ändern kann.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-724261.html

L-03 **Beckhoff: drei Lücken im Treiber TcRouter.sys geben lokalen Nutzern volle Systemrechte (CERT@VDE VDE-2026-087, 11.11.)**: Über offene IOCTL-Aufrufe im Treiber können lokale Nutzer oder Prozesse mit geringen Rechten auf physischen Speicher zugreifen und das Gerät vollständig übernehmen (CVE-2026-18767, CVE-2026-18768 und CVE-2026-18769, je CVSS 3.1: 7,8)

Relevanz: MITTEL

Betroffen ist TcRouter.sys für Windows (x64) in den im Advisory genannten Versionen. Betreiber sollten die Angaben zu betroffenen Versionen und Updates direkt im Advisory prüfen. Relevant ist das vor allem auf Industrie-PCs, an denen mehrere Personen arbeiten oder auf denen zusätzliche Software läuft, etwa für Fernwartung.

Quelle: https://certvde.com/en/advisories/VDE-2026-087/

L-04 **SANS 2026 State of ICS/OT Security Survey: 34 % der Befragten meldeten einen Vorfall (Pressemitteilung vom 10.11.)**: Im Vorjahr waren es 22 %, laut SANS der größte Anstieg innerhalb eines Jahres in der Geschichte der Umfrage. 72 % dieser Vorfälle haben den Betrieb gestört

Relevanz: MITTEL

Nur 15 % der Befragten können kritische Abläufe voll im Handbetrieb länger als 48 Stunden aufrechterhalten, 40 % wissen es nicht. Für Produktionsleiter heißt das: Den Handbetrieb für den Fall, dass SCADA oder DCS ausfallen, konkret planen und üben, nicht nur aufschreiben. Unsere Einordnung: Das ist ein Fall für CC1 ICS Incident Response der SANS Five ICS Critical Controls.

Quelle: https://www.sans.org/press/announcements/34-percent-industrial-organizations-suffered-cyber-incident-72-of-those-incidents-disrupted-operations-new-sans-institute-survey-finds

L-05 **Helmholz myREX24V2 und myREX24V2.virtual: zwölf Lücken, darunter XSS mit CVSS 9,3 (CERT@VDE VDE-2026-141, 10.11.)**: Laut CERT@VDE könnten die Lücken Remote Code Execution, DoS oder das Abfließen von Informationen erlauben

Relevanz: HOCH

Betroffen ist die Firmware vor 2.21.0 (CVE-2026-60035 bis CVE-2026-60046). Ohne Anmeldung möglich sind XSS gegen angemeldete Benutzer (CVE-2026-60043, CVSS 3.1: 9,3), CSRF (CVE-2026-60041, 8,1) und eine Passwort-Wiederherstellung ohne Rate Limiting (CVE-2026-60046, 7,5). Backups sind mit einem festen Passwort geschützt (CVE-2026-60044, 7,5). Wer hohe Rechte hat, kann über fünf Wege OS-Befehle einschleusen (je 7,2). Zu einer Ausnutzung sagt das Advisory nichts. myREX24 ist ein Fernwartungsportal, über das Maschinenbauer und Integratoren auf Anlagen ihrer Kunden zugreifen. Wer es selbst betreibt oder darüber Pumpwerke, Kläranlagen oder Maschinen in Bayern, Salzburg und Tirol fernwarten lässt, sollte das Update einplanen, am besten gleich auf 2.21.6 (siehe nächste Meldung). Das gehört zu CC4 Secure Remote Access der SANS Five ICS Critical Controls.

Quelle: https://www.certvde.com/en/advisories/VDE-2026-141/

L-06 □ UPDATE: **Helmholz myREX24V2 und myREX24V2.virtual: php2shell, Fix erst mit 2.21.6 (CERT@VDE VDE-2026-160, 10.11.)**: Betroffen ist die Firmware vor 2.21.6

Relevanz: HOCH

Die schwerere der beiden Lücken (CVE-2026-109619, CVSS 3.1: 8,1) ist ein Use After Free, der ohne Anmeldung über das Netz erreichbar ist. Die zweite (CVE-2026-109618, 5,3) kann den Dienst stören. Zu einer Ausnutzung sagt das Advisory nichts. Die zwölf Lücken aus der vorigen Meldung sind ab 2.21.0 behoben, ein Update auf 2.21.6 deckt also beide Advisories ab.

Quelle: https://www.certvde.com/en/advisories/VDE-2026-160/

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/