OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 10.11.2026, 16:32 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	10.11.2026
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 3 mit hoher Relevanz für Betreiber in DACH.

• **Update Kühlanlagen-Angriffe: Frankreich schreibt die Oktober-Angriffe einer Einheit der iranischen Revolutionsgarden zu (09.11.)**: Laut BleepingComputer ordnen die französischen Behörden die Angriffe in der Nacht vom 11. auf den 12

• **Siemens SIMATIC WinCC und PCS 7: Angreifer können Sitzungen übernehmen, für einige Produkte ist derzeit kein Fix geplant (SSA-970803, 10.11.)**: CVE-2026-58114 (CVSS 3.1: 7,5) nutzt die schwache NTLM-Anmeldung aus

• □ UPDATE: **Siemens „Node2Shell“ (CVE-2026-111497, CVSS 9,8) in BRAUMAT, SISTAR, WinCC OA, WinCC Unified, WinCC V7/V8 und weiteren Produkten (SSA-242944, 10.11.)**: Die Lücke steckt im Brotli-Decoder, den Siemens in diesen Produkten mitliefert, und kann Speicher beschädigen und eventuell die Ausführung von Code aus der Ferne erlauben

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**Update Kühlanlagen-Angriffe: Frankreich schreibt die Oktober-Angriffe einer Einheit der iranischen Revolutionsgarden zu (09.11.)**: Laut BleepingComputer ordnen die französischen Behörden die Angriffe in der Nacht vom 11. auf den 12	HOCH
L-02	**Siemens SIMATIC WinCC und PCS 7: Angreifer können Sitzungen übernehmen, für einige Produkte ist derzeit kein Fix geplant (SSA-970803, 10.11.)**: CVE-2026-58114 (CVSS 3.1: 7,5) nutzt die schwache NTLM-Anmeldung aus	HOCH
L-03	□ UPDATE: **Siemens „Node2Shell“ (CVE-2026-111497, CVSS 9,8) in BRAUMAT, SISTAR, WinCC OA, WinCC Unified, WinCC V7/V8 und weiteren Produkten (SSA-242944, 10.11.)**: Die Lücke steckt im Brotli-Decoder, den Siemens in diesen Produkten mitliefert, und kann Speicher beschädigen und eventuell die Ausführung von Code aus der Ferne erlauben	HOCH
L-04	**Siemens SIPROTEC 5: Jetzt gibt es auch für CP100-Geräte einen Fix (SSA-904646, Rev	MITTEL
L-05	**Bender EDGE500IP: Linux-Kernel-Lücken, die laut Advisory im CISA-KEV stehen (CERT@VDE VDE-2026-143, 10.11.)**: Betroffen ist COMTRAXX-Firmware 5.0.0 bis vor 5.1.1, mit CVE-2025-39682 (9,8) und CVE-2025-39964 (7,8)	MITTEL

Meldungen im Detail

L-01 **Update Kühlanlagen-Angriffe: Frankreich schreibt die Oktober-Angriffe einer Einheit der iranischen Revolutionsgarden zu (09.11.)**: Laut BleepingComputer ordnen die französischen Behörden die Angriffe in der Nacht vom 11. auf den 12

Relevanz: HOCH

Oktober auf Danfoss-Kühlsteuerungen der IRGC-nahen Einheit „Shahid Kaveh“ zu. Im Visier waren laut Behörden rund 700 Standorte im Einzelhandel. Getroffen wurden laut Quelle Supermarktketten, dazu kleinere Metzgereien, ein Schlachthof und genossenschaftliche Lebensmittelbetriebe. Mindestens 15 Brände werden den Angriffen zugeordnet. Die Zuordnung gilt nur für die Oktober-Angriffe in Frankreich, die späteren Wellen hat Frankreich ausdrücklich nicht dem Iran zugeschrieben. Im gleichen Zeitraum stellten die Ermittler laut Quelle Angriffe auf Schneider-Electric-Anlagen an kleinen Wasserkraftwerken fest, die sie derselben Kampagne zuordnen. Frankreich will den iranischen Botschafter einbestellen und neue EU-Sanktionen vorschlagen. Betreiber von Kühl- und Kälteanlagen in Lebensmittelbetrieben, Kliniken und Kühlhäusern in Bayern, Salzburg und Tirol sollten Hersteller-Fernzugänge jetzt auf offene Zugänge prüfen. (Die Erklärung des Ministeriums selbst habe ich nicht gefunden, Beleg ist nur die Presse.)

Quelle: https://bleepingcomputer.com/news/security/france-blames-iranian-hackers-for-supermarket-attacks-that-sparked-fires

L-02 **Siemens SIMATIC WinCC und PCS 7: Angreifer können Sitzungen übernehmen, für einige Produkte ist derzeit kein Fix geplant (SSA-970803, 10.11.)**: CVE-2026-58114 (CVSS 3.1: 7,5) nutzt die schwache NTLM-Anmeldung aus

Relevanz: HOCH

Ein Angreifer in einer Machine-in-the-Middle-Position kann die Sitzung eines Benutzers übernehmen und mit dessen Rechten Code ausführen. Betroffen sind alle Versionen von WinCC V7.5, V8.0 und V8.1, WinCC Runtime Professional V17 bis V21, PCS 7 V9.1, SIMATIC BATCH V9.1 sowie Process Historian und Information Server 2020 und 2022. Für WinCC und WinCC Runtime Professional gibt es noch keinen Fix, für PCS 7, BATCH, Process Historian und Information Server ist derzeit keiner geplant. Siemens rät, die Verbindung zum SQL Server zu verschlüsseln und wo möglich Kerberos statt NTLM zu nutzen. Wer WinCC oder PCS 7 in Leitwarten betreibt, etwa bei Wasser- und Abwasserbetrieben oder Stadtwerken, sollte die SQL-Verschlüsselung jetzt einplanen.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-970803.html

L-03 UPDATE: **Siemens „Node2Shell“ (CVE-2026-111497, CVSS 9,8) in BRAUMAT, SISTAR, WinCC OA, WinCC Unified, WinCC V7/V8 und weiteren Produkten (SSA-242944, 10.11.)**: Die Lücke steckt im Brotli-Decoder, den Siemens in diesen Produkten mitliefert, und kann Speicher beschädigen und eventuell die Ausführung von Code aus der Ferne erlauben

Relevanz: HOCH

Laut Advisory betroffen sind COMOS Walkinside, Project Server Web Administration Tool, SIMATIC BRAUMAT, SIMATIC Profiling Tool, SIMATIC SISTAR, WinCC Companion, WinCC OA V3.20 und V3.21, WinCC Runtime Professional, WinCC Unified (PC Runtime, Industrial Edge, SIQENCE), WinCC V7/V8, TIA Administrator und User Management Component (UMC). Bei BRAUMAT und SISTAR sind die Versionen ab V8.2 Update 1 betroffen, der Fix kommt mit V8.2 Update 5. Für WinCC OA V3.20 gibt es P17.1. Für alle anderen gibt es noch keinen Fix, für das Profiling Tool ist keiner geplant. Bis dahin rät Siemens, die Brotli-Kompression abzuschalten, bei TIA Administrator und UMC zusätzlich einen IIS-Filter gegen „br“ im Content-Encoding-Header zu setzen. Von einer Ausnutzung steht im Advisory nichts. Brauereien mit BRAUMAT und Betreiber von WinCC-Leitsystemen in DACH sollten das Update bzw. den Workaround in die nächste Wartung nehmen.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-242944.html

Quelle: https://ot-cyber.de/ot-lage/2026-10-31.html

L-04 **Siemens SIPROTEC 5: Jetzt gibt es auch für CP100-Geräte einen Fix (SSA-904646, Rev

Relevanz: MITTEL

V1.2 vom 10.11.)**: Über CVE-2025-40742 (CVSS 3.1: 5,3) können Sitzungsdaten aus Browser-Verlauf oder Logs abfließen. CP100-Geräte brauchen V8.91, CP150, CP300 und CP050 brauchen V11.0. Unsere Einschätzung: Das betrifft vor allem Stadtwerke und Verteilnetzbetreiber, die SIPROTEC 5 als Schutzgeräte im Umspannwerk einsetzen. Wer CP100-Geräte hat, sollte den Fix in die nächste Wartung einplanen.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-904646.html

L-05 **Bender EDGE500IP: Linux-Kernel-Lücken, die laut Advisory im CISA-KEV stehen (CERT@VDE VDE-2026-143, 10.11.)**: Betroffen ist COMTRAXX-Firmware 5.0.0 bis vor 5.1.1, mit CVE-2025-39682 (9,8) und CVE-2025-39964 (7,8)

Relevanz: MITTEL

Fix ist 5.1.1. Nach Bender ist die elektrische Sicherheit nicht betroffen. Ausnutzen lassen sich die Lücken nur, wenn ein Angreifer schon Code auf dem Gerät ausführen kann.

Quelle: https://certvde.com/en/advisories/VDE-2026-143/

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