OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 08.11.2026, 07:27 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	08.11.2026
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 2 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• **SonicWall-Firewalls: Lücke im SSL-VPN wird ausgenutzt (CVE-2026-19868, CISA-KEV seit 06.11.)**: Über CVE-2026-19868 in SonicOS SSL-VPN kann ein Angreifer mit gültigen Zugangsdaten für eine andere Anmeldeart an der SAML-Anmeldung vorbeikommen, möglicherweise auch an einer per SAML erzwungenen MFA

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**SonicWall-Firewalls: Lücke im SSL-VPN wird ausgenutzt (CVE-2026-19868, CISA-KEV seit 06.11.)**: Über CVE-2026-19868 in SonicOS SSL-VPN kann ein Angreifer mit gültigen Zugangsdaten für eine andere Anmeldeart an der SAML-Anmeldung vorbeikommen, möglicherweise auch an einer per SAML erzwungenen MFA	HOCH
L-02	UPDATE: **WAGO: CODESYS-Advisory überarbeitet, PFC300 jetzt auch betroffen (CERT@VDE VDE-2025-081, Rev. 1.1.0 vom 06.11.)**: Die Advisory zu drei CODESYS-Control-Lücken in WAGO-Steuerungen nennt jetzt zusätzlich die PFC300, das Bediengerät WP400 ist dafür herausgenommen	MITTEL

Meldungen im Detail

L-01 **SonicWall-Firewalls: Lücke im SSL-VPN wird ausgenutzt (CVE-2026-19868, CISA-KEV seit 06.11.)**: Über CVE-2026-19868 in SonicOS SSL-VPN kann ein Angreifer mit gültigen Zugangsdaten für eine andere Anmeldeart an der SAML-Anmeldung vorbeikommen, möglicherweise auch an einer per SAML erzwungenen MFA

Relevanz: HOCH

Laut SonicWall ist das SSL-VPN nur angreifbar, wenn die SAML-Anmeldung eingeschaltet ist. Der Hersteller prüft eine Meldung über mögliche Ausnutzung, die CISA hat die Lücke am 06.11. in ihren KEV-Katalog aufgenommen (Frist für US-Bundesbehörden: 20.11.). Betroffen sind Gen7-Firewalls (TZ, NSa, NSsp, NSv) mit SonicOS 7.3.3-7015 und älter sowie Gen8 mit 8.2.2-8015 und älter. Den Fix bringen SonicOS 7.3.4-7013 und 8.2.3-8015, einen Workaround gibt es nicht. Ob die Lücke schon vor dem Patch ausgenutzt wurde, ist offen. SonicWall-Firewalls dienen bei Stadtwerken und Wasserversorgern oft als VPN-Gateway für die Fernwartung. Für die Region: Wer bei kleinen Stadtwerken, Zweckverbänden oder Kläranlagen in Bayern, Salzburg oder Tirol die Fernwartung über SonicWall-SSL-VPN mit SAML laufen lässt, sollte patchen und die VPN-Logs auf auffällige Anmeldungen prüfen.

Quelle: https://www.securityweek.com/sonicwall-patches-exploited-sonicos-bug-that-weakens-vpn-logins/

L-02 □ UPDATE: **WAGO: CODESYS-Advisory überarbeitet, PFC300 jetzt auch betroffen (CERT@VDE VDE-2025-081, Rev. 1.1.0 vom 06.11.)**: Die Advisory zu drei CODESYS-Control-Lücken in WAGO-Steuerungen nennt jetzt zusätzlich die PFC300, das Bediengerät WP400 ist dafür herausgenommen

Relevanz: MITTEL

Laut Revisionshinweis hat CERT@VDE dabei auch Tippfehler in den CVSS-Werten korrigiert, frühere Angaben zu den Werten gelten also nicht mehr. Betroffen sind außerdem CC100, PFC100 G2, PFC200 G2, TP600 und der Edge Controller. Zwei Lücken lassen sich ohne Anmeldung über das Netz ausnutzen und können das Gerät lahmlegen (CVE-2025-41738, CVSS 7,5; CVE-2025-41739, CVSS 5,9). Bei der dritten kann eine manipulierte CODESYS-Projektdatei beim Öffnen Code im Benutzerkontext ausführen (CVE-2025-41700, CVSS 7,8). Den Fix bringt Firmware 4.10.0 (FW32), für Custom-Firmware hilft der WAGO-Support. Für die Region: WAGO PFC100, PFC200 und CC100 sind in der Fernwirktechnik von Wasser- und Abwasseranlagen in DACH weit verbreitet. Betreiber aller genannten Geräte, auch der PFC300, sollten prüfen, ob Firmware 4.10.0 oder höher läuft.

Quelle: https://certvde.com/en/advisories/VDE-2025-081/

Quelle: https://ot-cyber.de/ot-lage/2026-10-05.html

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