

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 04.10.2026, 16:38 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	04.10.2026
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.

- Update: Citrix NetScaler SAML-Zero-Day

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Update: Citrix NetScaler SAML-Zero-Day	HOCH
L-02	NIST-Entwurf SP 800-82 Rev. 4 und CISA/FBI-Merkblatt zu ICS-Integratoren	MITTEL

Meldungen im Detail

L-01 Update: Citrix NetScaler SAML-Zero-Day

Relevanz: **HOCH**

Citrix hat Patches für CVE-2026-88779 veröffentlicht (Buffer Overflow, CVSS4 8,7); laut heise kursiert offenbar bereits ein Exploit. Betroffen sind nur Geräte, die als SAML-SP oder SAML-IdP konfiguriert sind. Behoben ist die Lücke in 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS und 13.1-37.282 FIPS/NDcPP. Wichtig: Der Fix der Vorwoche (14.1-73.37) schützt nicht vor dieser neuen Lücke. Das Citrix-Advisory nennt Denial of Service, heise berichtet zusätzlich von möglicher Codeausführung; watchTowr hat die Schwachstelle nach eigenen Angaben reproduziert. Unsere Empfehlung: in der Konfiguration nach „add authentication samlAction“ bzw. „samIdPProfile“ suchen, betroffene Geräte – gerade wenn sie als Remote Access für die Fernwartung dienen – sofort auf die genannten Versionen bringen und die Logs auf Abstürze und Auffälligkeiten prüfen.

Quelle: <https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html>

Quelle: <https://www.heise.de/news/Netscaler-Admins-aufgepasst-Zero-Day-verursacht-Crashes-und-Codeausfuhrung-11474971.html>

L-02 NIST-Entwurf SP 800-82 Rev. 4 und CISA/FBI-Merkblatt zu ICS-Integratoren

Relevanz: **MITTEL**

NIST hat am 21.09.2026 einen überarbeiteten Entwurf seines OT-Sicherheitsleitfadens veröffentlicht. Er deckt jetzt ausdrücklich Wasser und Abwasser sowie Gebäudeautomation ab und wendet Zero-Trust-Prinzipien an; Kommentare sind bis 30.11.2026 möglich. CISA und FBI empfehlen in einem Merkblatt Least Privilege für ICS-Systemintegratoren und verweisen auf einen Fall von März bis April 2025, in dem Angreifer in das Netz eines US-Automatisierungsdienstleisters eingedrungen sind. Aus unserer Sicht betrifft das direkt die Fernwartung durch Dienstleister bei Stadtwerken und Maschinenbauern.

Quelle: <https://csrc.nist.gov/pubs/sp/800/82/r4/ipd>

Quelle: <https://www.securityweek.com/ot-security-guidance-nist-drafts-updated-guide-cisa-fbi-advise-on-ics-integrators/>

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