

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 06.10.2026, 16:13 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	06.10.2026
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 4 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

- Moxa MGate: kritische Lücke in Protokoll-Gateways (MPSA-269540, 02.10.)
- Update: Citrix NetScaler CVE-2026-88779 (CVSS 8,7)

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Moxa MGate: kritische Lücke in Protokoll-Gateways (MPSA-269540, 02.10.)	HOCH
L-02	Update: Citrix NetScaler CVE-2026-88779 (CVSS 8,7)	HOCH
L-03	Backdoor „ClingSTUN“ greift Edge-Geräte und Industrie-Router an	MITTEL
L-04	McCrary Institute: drei Prioritäten gegen KI-gestützte Angriffe auf KRITIS	MITTEL

Meldungen im Detail

L-01 Moxa MGate: kritische Lücke in Protokoll-Gateways (MPSA-269540, 02.10.)

Relevanz: HOCH

Moxa meldet zwei Schwachstellen in seinen MGate-Gateways. CVE-2026-86325 (CVSS 4.0: 9,4, kritisch) ist ein Stack-Overflow in der Kontoverwaltung: Schon ein Web-Konto mit reinen Leserechten reicht, um Zugangsdaten auszulesen, Speicher zu verändern oder das Gerät lahmzulegen. CVE-2026-86326 (CVSS 4.0: 8,6) erlaubt privilegierten Nutzern, Firmware ohne gültige Signatur einzuspielen. Betroffen sind u. a. MB3170/3270/3180/3280/3480/3660, die 5000er-Serie (5101-5119, 5216-5217), EIP3170/3270 und W5108/W5208. Moxa liefert je nach Modell Firmware-Updates (z. B. v4.7.1); eine Ausnutzung ist bisher nicht bekannt. MGate-Geräte sitzen in Wasser- und Energieanlagen oft genau zwischen Leittechnik und Feldebene: Firmware aktualisieren, Management-Oberfläche abschotten und Read-only-Konten prüfen (CC2 Defensible Architecture, CC5 Risk-Based Vulnerability Management).

Quelle: <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-269540-cve-2026-86325>

L-02 Update: Citrix NetScaler CVE-2026-88779 (CVSS 8,7)

Relevanz: **HOCH**

Zur Schwere der Lücke sind sich die Fachleute uneins. Citrix spricht nur von Denial of Service bei NetScaler ADC/Gateway mit SAML-Konfiguration. Kevin Beaumont meldet dagegen Angriffe auf schon gepatchte Honeypots, Malware-Downloads und Shell-Befehle im Benutzernamen-Feld. watchTowr hält den Bug für einen reinen DoS. Angreifer nutzen ihn aber wohl, um Geräte gezielt abstürzen zu lassen und so die Ausnutzung der älteren Lücken CVE-2026-88771/-88772 zu beschleunigen. Laut The Record warnen die USA und Australien gemeinsam; eine Primärquelle des ACSC fehlt noch. Die CISA verpflichtet US-Bundesbehörden zu Patch und forensischer Analyse. Die Frist endet am Mittwoch, 07.10. Für Stadtwerke heißt das: Patchen allein reicht nicht. NetScaler, über die der Remote Access ins Leitnetz läuft, auf Kompromittierung prüfen (Webshells, neue Konten, Sessions).

Quelle:

<https://www.securityweek.com/exploitation-of-citrix-netscaler-zero-day-hits-appliances-patched-days-earlier/>

Quelle: <https://therecord.media/us-australia-warn-of-latest-citrix-vulnerability>

Quelle:

<https://www.cisa.gov/news-events/alerts/2026/10/04/cisa-adds-one-known-exploited-vulnerability-catalog>

L-03 Backdoor „ClingSTUN“ greift Edge-Geräte und Industrie-Router an

Relevanz: **MITTEL**

FortiGuard Labs hat am 05.10. eine Linux-Backdoor beschrieben. Sie verbreitet sich selbst und nutzt rund zwei Dutzend bekannte, ungepatchte Lücken aus, u. a. in Lantronix EDS5000 (CVE-2025-67038), Hytec-Inter HWL-2511-SS (CVE-2022-36553), Linear eMerge (CVE-2019-7256), Sunhillo SureLine (CVE-2021-36380) sowie bei D-Link, TP-Link, Ivanti und Realtek. Ihren C2-Verkehr versteckt sie über öffentliche STUN-Server. Solche Device-Server und Industrierouter stecken in DACH oft in Fernwirk- und Fernwartungs-Strecken. Deshalb das Asset-Inventar auf diese Modelle prüfen und ausgehenden Verkehr überwachen, auch STUN/UDP 3478.

Quelle:

<https://www.fortinet.com/blog/threat-research/clingstun-linux-backdoor-abuses-public-stun-infrastructure>

Quelle: <https://www.securityweek.com/linux-backdoor-abuses-stun-protocol-exploits-dozens-of-flaws/>

L-04 McCrary Institute: drei Prioritäten gegen KI-gestützte Angriffe auf KRITIS

Relevanz: **MITTEL**

Das Institut warnt, dass KI die Angriffe auf OT in kritischen Infrastrukturen beschleunigt, und nennt drei Prioritäten für die Abwehr. Die Details sind nicht belegt, weil die Seite nicht abrufbar war. Für Versorger in DACH ist der Bericht ein weiteres Argument, OT-Monitoring und Segmentierung jetzt anzugehen und nicht erst vor der NIS2-Prüfung.

Quelle: <https://industrialcyber.co/ai/mccrary-institute-outlines-three-priorities-for-defending-critical-infrastructure-against-ai-enabled-cyberattacks/>

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