

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 02.10.2026, 09:17 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	02.10.2026
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 8 Meldungen, davon 3 mit hoher Relevanz für Betreiber in DACH.

- Cisco Catalyst SD-WAN Manager: Zero-Day wird aktiv ausgenutzt (CVE-2026-76504, CVSS 9.8)
- WatchGuard Fireware OS: kritische Root-RCE und SSLVPN-Bypass
- TeamViewer: fünf Lücken bis CVSS 8.8 (CVE-2026-92370 u. a., Bulletin TV-2026-1010)

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Cisco Catalyst SD-WAN Manager: Zero-Day wird aktiv ausgenutzt (CVE-2026-76504, CVSS 9.8)	HOCH
L-02	WatchGuard Fireware OS: kritische Root-RCE und SSLVPN-Bypass	HOCH
L-03	TeamViewer: fünf Lücken bis CVSS 8.8 (CVE-2026-92370 u. a., Bulletin TV-2026-1010)	HOCH
L-04	ABB PCM600: Rechteausweitung und Path Traversal ohne Patch (CISA ICSA-26-274-03, 01.10.)	MITTEL
L-05	Monta monta.app (Lade-Backend): Ladestationen lassen sich ohne Anmeldung imitieren (CISA ICSA-26-274-02, 01.10.)	MITTEL
L-06	Armatura One (Zutrittskontrolle): alte ActiveMQ-Lücke und fest eingebaute Schlüssel (CISA ICSA-26-274-01, 01.10.)	MITTEL
L-07	Google GTIG: KI verdoppelt die Zahl gemeldeter Schwachstellen	MITTEL
L-08	Johnson Controls EasyIO Neo (Gebäudeautomation): Zugangsdaten im Klartext (CISA ICSA-26-274-04/-05, 01.10.)	MITTEL

Meldungen im Detail

L-01 Cisco Catalyst SD-WAN Manager: Zero-Day wird aktiv ausgenutzt (CVE-2026-76504, CVSS 9.8)

Relevanz: **HOCH**

Über eine speziell kodierte URL (`/%6a\_security\_check`) umgehen Angreifer ohne Anmeldung die Authentifizierung und nutzen die API mit Admin-Rechten. Die Lücke wird seit September angegriffen und ist der fünfte ausgenutzte Cisco-Zero-Day in diesem Jahr. Cisco hat sie am 30.09. veröffentlicht, CISA hat sie am selben Tag in den KEV-Katalog aufgenommen (Frist für US-Bundesbehörden: 03.10.). Einen Workaround gibt es nicht. Gepatcht sind 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 und 26.2.1. Stadtwerke und Netzbetreiber, die Leitstellen, Außenstellen oder Netzleittechnik über SD-WAN verbinden, sollten sofort patchen. Danach serviceproxy-access.log und vmanage-server.log nach `/%6a\_security\_check` durchsuchen.

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>

Quelle:

<https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog>

Quelle:

<https://helpnetsecurity.com/2026/10/01/new-cisco-sd-wan-zero-day-exploited-in-the-wild-cve-2026-76504>

L-02 WatchGuard Fireware OS: kritische Root-RCE und SSLVPN-Bypass

Relevanz: **HOCH**

Die schwerste Lücke ist CVE-2026-86131 (CVSS 9.2) im BOVPN-over-TLS-Client. Sie greift nur, wenn die Firebox sich mit einem VPN-Server verbindet, den der Angreifer kontrolliert. Dazu kommen ein Pre-Auth-DoS (CVE-2026-86134) und ein SAML-Bypass für SSLVPN (CVE-2026-86101). Ausgenutzt wird bisher nichts. WatchGuard hat die Lücken am 29.09. veröffentlicht. Wie viele es sind, ist unklar: heise zählt 15 und nennt zusätzlich 12.11.10 als Fix-Version, SecurityOnline zählt 14. Die Fireboxen trennen bei kleineren Stadtwerken häufig IT und OT oder stecken im Remote Access, deshalb auf 2026.3.2, 2026.2.3, 12.12.3 oder 12.5.21 aktualisieren.

Quelle:

<https://www.heise.de/news/WatchGuard-schliesst-teils-kritische-Luecken-in-Fireware-OS-11472101.html>

Quelle: <https://www.esecurityplanet.com/news/news-watchguard-fireware-root-flaw/>

L-03 TeamViewer: fünf Lücken bis CVSS 8.8 (CVE-2026-92370 u. a., Bulletin TV-2026-1010)

Relevanz: **HOCH**

Betroffen sind Full Client und Host vor 15.82 unter Windows, Linux und macOS. Die Lücken reichen von einer Code-Injektion, die die Rechte für eingehende Sessions umgeht, über Rechteauserweiterung auf SYSTEM/root bis zu einem Heap-Overflow beim Öffnen von .tvs-Aufzeichnungen. Ausgenutzt wird bisher nichts. Das Bulletin ist vom 29.09., heise berichtete am 01.10. Auf Kläranlagen, Wasserwerken und HMI-/SCADA-Rechnern läuft TeamViewer oft als Fernwartung von Dienstleistern. Deshalb den Bestand inklusive der Dienstleister-Installationen prüfen und auf 15.82 aktualisieren (Legacy-Patches gibt es für 13.2, 14.7 und 15.64). Dabei auch klären, ob die Hosts in der OT überhaupt nötig sind.

Quelle: <https://www.teamviewer.com/en-us/resources/trust-center/security-bulletins/tv-2026-1010/>

Quelle: <https://www.heise.de/news/TeamViewer-Codeschmuggel-Luecke-verpasst-nur-knapp-kritische-Einstufung-11472313.html>

Quelle: <https://www.heise.de/en/news/TeamViewer-patches-code-injection-vulnerability-11432925.html>

L-04 ABB PCM600: Rechteausweitung und Path Traversal ohne Patch (CISA ICSA-26-274-03, 01.10.)

Relevanz: MITTEL

Betroffen ist PCM600 bis 2.14. Bei CVE-2026-15952 (CVSS v4 7.1) läuft der Scheduler-Dienst als LocalSystem, Standardnutzer können darüber ihre Rechte ausweiten. CVE-2026-15953 erlaubt beim Entpacken von Archiven das Schreiben außerhalb des Zielordners. Ausgenutzt wird bisher nichts. Mit PCM600 konfigurieren viele Verteilnetzbetreiber in DACH die Relion-Schutzgeräte in Umspannwerken und Ortsnetzstationen. Einen Fix gibt es nicht. Deshalb den Dienst unter dem PCM600-Konto statt als LocalSystem betreiben (ABB-Advisories 2NGA003170 und 2NGA003179) und die Engineering-Rechner strikt segmentieren.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-03>

L-05 Monta monta.app (Lade-Backend): Ladestationen lassen sich ohne Anmeldung imitieren (CISA ICSA-26-274-02, 01.10.)

Relevanz: MITTEL

Vier Lücken betreffen alle Versionen. Die schwerste ist CVE-2026-95102 (CVSS 9.4): Die WebSocket-Endpunkte verlangen keine Authentifizierung. Mit Stations-IDs aus öffentlichen Ladekarten kann man sich als Ladesäule ausgeben und Sessions kapern. Dazu kommen vorhersagbare Session-IDs und offen liegende Zugangsdaten der Ladestationen. CISA nennt Energie und Transport als betroffene Sektoren. Stadtwerke, die ihre Ladeinfrastruktur über Monta betreiben, sollten OCPP 1.6 Security Profile 2 (Basic Auth über TLS) erzwingen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>

Quelle: <https://securityonline.info/monta-ev-charging-vulnerabilities/>

L-06 Armatura One (Zutrittskontrolle): alte ActiveMQ-Lücke und fest eingebaute Schlüssel (CISA ICSA-26-274-01, 01.10.)

Relevanz: MITTEL

Das Produkt enthält ein verwundbares Apache ActiveMQ mit CVE-2023-46604 (CVSS 9.8), das Ransomware-Gruppen seit Jahren ausnutzen. Außerdem gibt es einen hartcodierten Schlüssel, ein Standard-Passwort für die Datenbank und Zugangsdaten im Klartext in den Logs. Bei KRITIS-Betreibern sichert die Zutrittskontrolle Anlagen und Leitwarten, hängt aber oft im IT-Netz. Deshalb auf v4.7.2 bzw. v4.6.1_USA aktualisieren.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-01>

L-07 Google GTIG: KI verdoppelt die Zahl gemeldeter Schwachstellen

Relevanz: MITTEL

Laut dem Bericht vom 30.09. stiegen die Meldungen von 5.045 im Januar auf 10.740 im August 2026. Ausgenutzt werden im Schnitt 18 Lücken pro Monat, 2025 waren es 10,5. Von den vermutlich durch KI gefundenen Lücken führen 50 % zu RCE, bei den übrigen sind es 26 %. 14 % der ausgenutzten Lücken betreffen Edge Devices und Security-Appliances. Für die Daseinsvorsorge heißt das: Die Zeit zum Patchen von Firewalls und VPN-Gateways wird weiter kürzer.

Quelle: <https://cloud.google.com/blog/topics/threat-intelligence/vulnerability-discovery-and-exploitation-trends-in-the-ai-era/>

Quelle: <https://siliconangle.com/2026/09/30/google-finds-vulnerability-disclosures-doubled-as-ai-changes-which-flaws-get-discovered/>

L-08 Johnson Controls EasyIO Neo (Gebäudeautomation): Zugangsdaten im Klartext (CISA ICSA-26-274-04/-05, 01.10.)

Relevanz: MITTEL

Zwei Lücken betreffen die Controller der EC- und CW-Serie. Über CVE-2026-64893 (CVSS 5.4) lassen sich Zugangsdaten und Sessions per HTTP mitlesen, CVE-2026-64892 gibt sensible Daten preis. Behoben ist das in Firmware EC V3.3b64 bzw. CW V3.3b26, dort ist HTTP standardmäßig abgeschaltet. Die Bewertung ist niedrig, wichtig wird es, wenn die Gebäudeleittechnik von Betriebsgebäuden, Leitstellen oder Wasserwerken im selben Netz wie die OT hängt. Dann HTTP abschalten und das GLT-Netz segmentieren.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-05>

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-04>

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