

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 03.10.2026, 16:11 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	03.10.2026
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.

- Citrix NetScaler: neuer Zero-Day trifft auch gepatchte Geräte
- Warlock-Ransomware trifft einen Wasserversorger über alte SharePoint-Lücken
- Fortinet FortiMail: Zero-Day ohne Anmeldung wird ausgenutzt, Patch fehlt noch

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Citrix NetScaler: neuer Zero-Day trifft auch gepatchte Geräte	HOCH
L-02	Warlock-Ransomware trifft einen Wasserversorger über alte SharePoint-Lücken	HOCH
L-03	Fortinet FortiMail: Zero-Day ohne Anmeldung wird ausgenutzt, Patch fehlt noch	HOCH
L-04	CODESYS: zwei Lücken in Gateway und Control Runtime, BSI-Warnung vom 02.10.	MITTEL
L-05	WatchGuard Fireware OS: 15 Lücken in den Firewalls, eine kritisch	MITTEL
L-06	ABB PCM600: Rechteausweitung im Engineering-Tool für Schutzgeräte (CISA ICISA-26-274-03, 01.10.)	MITTEL
L-07	Johnson Controls EasyIO Neo: Zugangsdaten gehen im Klartext übers Netz (CISA ICISA-26-274-04/-05, 01.10.)	MITTEL
L-08	TDengine: Ein einziges Paket bringt die Zeitreihen-Datenbank zum Absturz (CVE-2026-42542, CVSS 7,5)	MITTEL

Meldungen im Detail

L-01 Citrix NetScaler: neuer Zero-Day trifft auch gepatchte Geräte

Relevanz: **HOCH**

Seit dem Abend des 02.10. wird eine weitere Lücke ausgenutzt. Laut Kevin Beaumont bringen massenhaft gesendete SAML-Anfragen die Geräte zum Absturz oder führen Code aus. Seine Honeypots waren bereits gegen CVE-2026-88771/-88772 gepatcht und bekamen trotzdem Webshells. Eine CVE und einen Patch gibt es noch nicht. Citrix bestätigt ein eigenständiges Problem bei Gateway/AAA mit SAML-Anmeldung und verweist bisher nur an den Support. Wer NetScaler für den Fernzugang von Dienstleistern oder Leitstellen nutzt, sollte die SAML-Konfiguration prüfen, nach Webshells suchen und den Zugang notfalls vom Netz nehmen.

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

L-02 Warlock-Ransomware trifft einen Wasserversorger über alte SharePoint-Lücken

Relevanz: **HOCH**

Symantec hat am 01.10. gemeldet, dass die China-nahe Gruppe Longlegs (Storm-2603) in den letzten zwei Monaten mindestens vier Organisationen angegriffen hat, darunter einen Wasserversorger und einen Telekommunikationsanbieter. The Record hat am 02.10. darüber berichtet. Die Opfer liegen in spanisch- und portugiesischsprachigen Ländern in Europa, Afrika und Lateinamerika. Der Einstieg lief über die „ToolShell“-Lücken in On-Premises-SharePoint (CVE-2025-49704, -49706, -53770, -53771). Vom ersten Webshell-Zugriff am 22.07. bis zur Verschlüsselung vergingen etwa zehn Tage. Am 31.07. waren dann innerhalb von zwei Stunden mehr als 33 Rechner verschlüsselt. Vorher hatten die Angreifer auf mindestens 40 Systemen die Sicherheitssoftware abgeschaltet. Auswirkungen auf die OT nennt Symantec ausdrücklich nicht. Für Versorger in DACH heißt das: SharePoint-Server vor Ort, auf denen oft die Anlagendokumentation liegt, patchen oder vom Internet nehmen und die Segmentierung zwischen IT und OT prüfen.

Quelle: <https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>

Quelle: <https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks>

L-03 Fortinet FortiMail: Zero-Day ohne Anmeldung wird ausgenutzt, Patch fehlt noch

Relevanz: **HOCH**

Über CVE-2026-104286 (CVSS 9,8, FG-IR-26-175) können Angreifer ohne Anmeldung beliebige Dateien schreiben und Code ausführen. Betroffen sind die Zweige 7.2 bis 8.0. CISA hat die Lücke am 01.10. in den KEV-Katalog aufgenommen. Bis zum Update hilft nur, die IBE-Funktion abzuschalten und das Management-Interface aus dem Internet zu nehmen. Bei Stadtwerken ist FortiMail oft das zentrale Mail-Gateway und damit ein guter Startpunkt für Phishing und Lateral Movement Richtung OT. Die Meldung ist seit 01.10. bekannt und stand möglicherweise schon in einem früheren Briefing.

Quelle: <https://www.heise.de/news/FortiMail-Angriffe-auf-Zero-Day-Luecke-laufen-Workaround-verfuegbar-11473599.html>

L-04 CODESYS: zwei Lücken in Gateway und Control Runtime, BSI-Warnung vom 02.10.

Relevanz: **MITTEL**

Mit CVE-2026-76992 (CVSS 7,5) kann ein bössartiges Gateway den Gateway Client ohne Anmeldung per Speicherüberlauf lahmlegen. Das betrifft auch das Development System und HMI. Mit CVE-2026-79625 (CVSS 8,1) kann ein angemeldeter Nutzer mit Monitoring-Rechten über eine Race Condition Speicher in der SPS-Runtime beschädigen. CODESYS steckt in vielen Steuerungen in DACH-Anlagen, zum Beispiel bei WAGO und auf Linux- oder Raspberry-Pi-Runtimes. Für diese Runtimes kommt der Fix (Version 4.23.0.0) erst im 4. Quartal. Bis dahin sollte nur geprüfte Engineering-Hardware Zugang haben, und das Monitoring sollte auf wenige Konten beschränkt werden.

Quelle: <https://certvde.com/en/advisories/VDE-2026-094/>

L-05 WatchGuard Fireware OS: 15 Lücken in den Firewalls, eine kritisch

Relevanz: MITTEL

CVE-2026-86131 (CVSS 9,2) erlaubt Remote Code Execution über den BOVPN-over-TLS-Client. Dazu kommen Buffer Overflows und ein SAML-Auth-Bypass. Ausgenutzt wird bisher nichts. Bei Zweckverbänden sichern diese Firewalls oft die Grenze zwischen IT und OT oder die VPN-Strecken zu Außenstellen, deshalb sollten sie zügig aktualisiert werden.

Quelle:

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

L-06 ABB PCM600: Rechteausweitung im Engineering-Tool für Schutzgeräte (CISA ICSA-26-274-03, 01.10.)

Relevanz: MITTEL

Betroffen sind Version 2.14 und älter (CVE-2026-15952, CVSS v4 7,1, und CVE-2026-15953, CVSS v4 5,6). Angreifer können sich höhere Rechte verschaffen oder per Path Traversal Dateien überschreiben. Einen Patch nennt die Advisory nicht, nur Konfigurationsmaßnahmen: den Scheduler-Dienst unter dem PCM600-Konto betreiben und die IED-Authentifizierung aktivieren. PCM600 ist bei Netzbetreibern und Stadtwerken für Schutz- und Leittechnik nach IEC 61850 verbreitet, deshalb sollten die Engineering-Stationen gehärtet werden.

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

L-07 Johnson Controls EasyIO Neo: Zugangsdaten gehen im Klartext übers Netz (CISA ICSA-26-274-04/-05, 01.10.)

Relevanz: MITTEL

Bei den Controllern EC (V3.3b62/63) und CW (V3.3b24/25) laufen Zugangsdaten und Session-Daten unverschlüsselt über HTTP (CVE-2026-64893, CVSS 5,4). Eine zweite Lücke (CVE-2026-64892) legt sensible Informationen offen. Behoben ist das in EC V3.3b64 und CW V3.3b26. Betroffen ist die Gebäudeautomation in Betriebsgebäuden, Leitstellen und Klärwerken, die oft per Fernwartung von Dienstleistern betreut wird.

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>

L-08 TDengine: Ein einziges Paket bringt die Zeitreihen-Datenbank zum Absturz (CVE-2026-42542, CVSS 7,5)

Relevanz: MITTEL

Ein Integer-Underflow in der RPC-Verarbeitung erlaubt schon vor der Anmeldung einen Denial of Service über TCP 6030. Betroffen sind die Versionen 3.4.0.0 bis 3.4.1.5, behoben ist es in 3.4.1.6. Es gibt einen Proof of Concept, ausgenutzt wird die Lücke laut RedSeal bisher nicht. TDengine dient in Energie- und Versorgungsumgebungen als Historian. Fällt er aus, verliert die Leitstelle die Sicht auf ihre Anlagen. Die Lücke wurde schon am 29.09. veröffentlicht, ist also älter als 24 Stunden.

Quelle: <https://www.redseal.net/tdengine-cve-2026-42542-ot-iot-security/>

Quelle: <https://app.openCVE.io/cve/CVE-2026-42542>

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