OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 01.11.2026, 07:35 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	01.11.2026
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 3 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• Ransomware-Gruppe „The Gentlemen“ nennt den Wassertechnik-Konzern WABAG als Opfer (erfasst am 31.10.)

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Ransomware-Gruppe „The Gentlemen“ nennt den Wassertechnik-Konzern WABAG als Opfer (erfasst am 31.10.)	HOCH
L-02	TeamViewer: Ein manipulierter Zielrechner kann den Rechner des Verbindenden angreifen (CVE-2026-111585, CVSS 8,8, Bulletin TV-2026-1011 vom 27.10., aktualisiert 28.10.)	MITTEL
L-03	Update: Ivanti Connect Secure, CISA nimmt zwei weitere Lücken der Angriffskette in den KEV-Katalog auf (30.10.)	MITTEL

Meldungen im Detail

L-01 Ransomware-Gruppe „The Gentlemen“ nennt den Wassertechnik-Konzern WABAG als Opfer (erfasst am 31.10.)

Relevanz: HOCH

Der Leak-Site-Tracker ransomware.live hat den Eintrag „WABAG“ (Domain wabag.in, Indien) am 31.10. um 07:27 UTC erfasst. Als geschätztes Angriffsdatum („Est. attack date“) nennt er den 26.10. In den dort eingebundenen Infostealer-Daten zählt Hudson Rock 76 WABAG-Mitarbeiter mit Infostealer-Infektion, ein Zusammenhang mit dem Angriff ist nicht belegt. Bisher ist das nur eine Angabe der Gruppe. Eine Stellungnahme von WABAG (Firmenseite, Pressemitteilung) habe ich bis 01.11. nicht gefunden, zu Datenmenge oder Betriebsfolgen gibt es keine Angaben. Laut Firmenprofil auf wabag.com hat die WABAG-Gruppe ihren Hauptsitz in Chennai, ist in mehr als 25 Ländern vertreten und arbeitet unter anderem in Trinkwasseraufbereitung, Abwasserbehandlung, industrieller Wasseraufbereitung und Entsalzung. Bezug zu Österreich: Im Firmenbuch ist unter FN 93654b die VA TECH WABAG GmbH mit Sitz in Wien eingetragen, einzige eingetragene Gesellschafterin ist die VA TECH WABAG (Singapore) Pte. Ltd. Ob die Wiener Gesellschaft betroffen ist, ist offen. Meine Einschätzung (Max Gilg): Betreiber, die mit WABAG Projekte oder Wartungsverträge haben, sollten jetzt prüfen, welche Anlagendokumentation und welche Fernzugänge beim Dienstleister liegen, und Zugangsdaten für den Remote Access vorsorglich tauschen.

Quelle: https://www.ransomware.live/id/V0FCQUdAdGhlZ2VudGxlbWVu

Quelle: https://www.wabag.com/company/

Quelle: https://www.evi.gv.at/f/93654b

L-02 TeamViewer: Ein manipulierter Zielrechner kann den Rechner des Verbindenden angreifen (CVE-2026-111585, CVSS 8,8, Bulletin TV-2026-1011 vom 27.10., aktualisiert 28.10.)

Relevanz: MITTEL

Verbindet sich ein Nutzer mit einem vom Angreifer kontrollierten oder kompromittierten Host, kann ein Integer Overflow bei der Verarbeitung der Bildschirmdaten den Viewer abstürzen lassen oder je nach Plattform Code mit den Rechten des Viewers ausführen. Betroffen sind Full Client und Portable vor 15.83 (Windows, Linux, macOS) sowie die Android-App Remote Control vor 15.83. Im selben Bulletin stehen CVE-2026-92372 (CVSS 8,8, Out-of-Bounds Write im Bilddecoder, Linux und macOS) und CVE-2026-92374 (CVSS 7,8, Root-Rechte unter macOS). Behoben in 15.83, für ältere Versionen gibt es eigene Legacy-Builds. Laut TeamViewer ist keine aktive Ausnutzung bekannt. Meine Einschätzung (Max Gilg): TeamViewer ist in der Fernwartung von Anlagen verbreitet. Ein kompromittiertes HMI oder ein kompromittierter Anlagen-PC könnte so den Laptop des Servicetechnikers übernehmen, deshalb auch die Servicelaptops der Dienstleister auf 15.83 bringen.

Quelle: https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2026-1011/

L-03 Update: Ivanti Connect Secure, CISA nimmt zwei weitere Lücken der Angriffskette in den KEV-Katalog auf (30.10.)

Relevanz: MITTEL

Der von Volexity als UTA0576 bezeichnete Threat Actor nutzt laut Volexity seit dem 3.10. Lücken in Ivanti Connect Secure in Kombination und erreicht so laut Volexity Codeausführung als Root ohne Anmeldung. Laut The Hacker News gehören CVE-2026-104935, CVE-2026-111357 und CVE-2026-118527 zur Kette. Volexity fand auf dem Gerät weder Webshell noch Backdoor, die Befehle liefen über die Exploit-Kette selbst. Abgegriffen wurden auf dem Gerät gespeicherte Zugangsdaten, etwa die für LDAP genutzten Domänen-Zugangsdaten, dazu AD-Metadaten. Mit einem eigenen LDAP-Tool suchte der Angreifer im Active Directory gezielt nach LAPS-Passwörtern und BitLocker-Recovery-Keys. Laut Volexity erkennt der Integrity Checker die Kompromittierung womöglich nicht. CISA hat am 30.10. CVE-2026-111357 („Missing Authentication for Critical Function“) und CVE-2026-118527 („Generation of Predictable Numbers or Identifiers“) in den KEV-Katalog aufgenommen. Laut The Hacker News sind die Fixes 25.1.1.3 und 22.8R2.6. Meine Einschätzung (Max Gilg): Wer den VPN-Zugang ins OT-Netz über Ivanti betreibt, sollte patchen und das LDAP-Dienstkonto, LAPS-Passwörter und BitLocker-Keys vorsorglich tauschen.

Quelle: https://www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/

Quelle: https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog

Quelle: https://thehackernews.com/2026/10/attackers-chain-three-ivanti-connect.html

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