OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 31.10.2026, 16:10 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	31.10.2026
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.

• Stadtwerke Waldbröl (NRW) erpresst, Kundendaten abgeflossen: Laut Oberberg-Aktuell vom 30.10. wurden die Stadtwerke rund drei Wochen vor dem Bericht erpresst, die Täter drohten mit der Veröffentlichung von Kundendaten. Geschäftsführer Mirco Kujbida spricht von einer „finanziell motivierten, russischen Hackerbande“. Das Unternehmen beauftragte IT-Forensiker, laut Unternehmen wurden tatsächlich Daten gestohlen. Wie viele Kunden betroffen sind, steht laut Bericht noch nicht fest. Versorgung und Erreichbarkeit waren laut Kujbida zu keinem Zeitpunkt unterbrochen oder gefährdet, die Sicherheitslücke ist laut Artikel behoben, das LKA ermittelt. Einen Gruppennamen und den Angriffsweg nennt der Bericht nicht. Wir haben dazu nur diese eine Quelle gefunden. Unsere Einschätzung: Auch ohne Eingriff in die Leittechnik bleibt für Stadtwerke die Erpressung mit Kundendaten ein reales Risiko, Incident Response und Meldewege sollten dafür geübt sein. Quelle: https://www.oberberg-aktuell.de/blaulicht/stadtwerke-wurden-von-russischer-hackerbande-erpresst-a-139763

• □ UPDATE: Brotli-Lücke CVE-2026-111497 trifft Siemens Industrial Edge, für sieben Management-Apps gibt es noch keinen Fix (SSA-443410 vom 30.10.): Siemens nennt im Advisory CVSS v3.1 9,8 und CVSS v4.0 9,2. Die Industrial Edge Management Cloud ist laut Siemens seit 28.10. zentral gefixt, der Industrial Edge Hub seit 29.10., Anwender müssen dort nichts tun. Ohne Fix sind Cloud Connector Configurator, Common Configurator on Device (CC on Edge), Common Configurator (CC on IEM), Data Flow Monitoring, Databus Configurator, Edge OPC UA Server Configurator und Flow Creator Configurator. Siemens empfiehlt bis zum Fix, CC on Edge und Data Flow Monitoring zu stoppen; für die übrigen Apps alle Management Applications zu deinstallieren und die IEM-Instanz per Firewall/WAF zu schützen. Sind keine Management Applications installiert, ist laut Siemens nichts zu tun. Die CISA führt die Lücke in der Brotli-Bibliothek von Google seit 27.10. im KEV-Katalog, also als ausgenutzt (Frist für US-Behörden 10.11.). Für Betreiber, die Industrial Edge in Wasser- oder Energieanlagen einsetzen, heißt das: installierte Management-Apps prüfen und die Maßnahmen von Siemens umsetzen. Dieselbe Lücke betrifft laut SSA-898633 (30.10.) auch RUGGEDCOM APE1808 mit PAN-OS, eine Siemens-Plattform für Edge Computing und Cybersecurity in rauen Industrieumgebungen, auf der die Firewall-Software von Palo Alto Networks läuft. Siemens nennt dort keine konkrete Fix-Version und verweist auf das passende PAN-OS-Upgrade. Laut Palo Alto Networks betrifft die Lücke bei PAN-OS nur PA- und VM-Series-Firewalls, die Brotli-komprimierten Traffic prüfen und TLS/SSL-Decryption auf der Dataplane aktiv haben; die Management-Oberfläche (Web oder API) ist nicht betroffen. Gefixt ist PAN-OS ab 12.2.4-h1, 12.1.4-h13, 12.1.7-h11, 12.1.10-h3 sowie 11.2.4-h23, 11.2.7-h23, 11.2.10-h17, 11.2.13-h4 und 11.2.16-h1, PAN-OS 11.1 und 10.2 sind nicht betroffen. Als Workaround nennt Palo Alto Networks, die Brotli-Inspektion per CLI abzuschalten; ab PAN-OS 11.2.4 ist Brotli-Encoding standardmäßig aus. Eine Ausnutzung bei PAN-OS ist Palo Alto Networks laut eigenem Advisory nicht bekannt. Quellen: https://productcert.siemens.com/productcert/html/ssa-443410.html · https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json · https://productcert.siemens.com/productcert/html/ssa-898633.html · https://security.paloaltonetworks.com/CVE-2026-111497 (Erstmeldung am 28.10.2026: https://ot-cyber.de/ot-lage/2026-10-28.html)

• Ivanti Connect Secure: zwei ausgenutzte Lücken seit 30.10. im KEV-Katalog der CISA: Die CISA führt CVE-2026-111357 als „Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability“ und CVE-2026-118527 als „Ivanti Connect Secure Generation of

Predictable Numbers or Identifiers Vulnerability“. Die Beschreibungen von CVE-2026-111357 weichen voneinander ab: Der KEV-Kasten bei SecurityOnline nennt für Version 22.8R2.4 einen Fehler im dsinvoked-Broker, der DSCache-Konfigurationsdaten vertraut (CVSS 7,0), der Artikeltext derselben Seite nennt fehlende Authentifizierung mit Rechteausweitung bis root und CVSS 8,8. CVE-2026-118527 betrifft laut SecurityOnline vorhersehbare Dateinamen: Ein angemeldeter Angreifer kann Schaddateien an bekannte Orte auf dem Gerät ablegen. Laut SecurityOnline nutzen Angreifer beide Lücken in einer Kette mit CVE-2026-104935 (Umgehung der Authentifizierung), um Root-Rechte zu bekommen. Das Ivanti-Advisory selbst konnten wir nicht prüfen. Für Betreiber, die Ivanti als VPN für die Fernwartung nutzen, heißt das: auf die Fix-Versionen aus dem Ivanti-Advisory aktualisieren (SecurityOnline nennt im Abschnitt zur Mitigation 25.1.1.3, 25.1.3.1 und 22.8R2.6, die Tabelle derselben Seite weicht davon ab), das Integrity Checker Tool von Ivanti laufen lassen, Logs prüfen und Zugangsdaten zurücksetzen, weil ein Patch bereits gestohlene Daten nicht ungültig macht. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://securityonline.info/ivanti-connect-secure-vulnerability-exploited/

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Stadtwerke Waldbröl (NRW) erpresst, Kundendaten abgeflossen: Laut Oberberg-Aktuell vom 30.10. wurden die Stadtwerke rund drei Wochen vor dem Bericht erpresst, die Täter drohten mit der Veröffentlichung von Kundendaten. Geschäftsführer Mirco Kujbida spricht von einer „finanziell motivierten, russischen Hackerbande“. Das Unternehmen beauftragte IT-Forensiker, laut Unternehmen wurden tatsächlich Daten gestohlen. Wie viele Kunden betroffen sind, steht laut Bericht noch nicht fest. Versorgung und Erreichbarkeit waren laut Kujbida zu keinem Zeitpunkt unterbrochen oder gefährdet, die Sicherheitslücke ist laut Artikel behoben, das LKA ermittelt. Einen Gruppennamen und den Angriffsweg nennt der Bericht nicht. Wir haben dazu nur diese eine Quelle gefunden. Unsere Einschätzung: Auch ohne Eingriff in die Leittechnik bleibt für Stadtwerke die Erpressung mit Kundendaten ein reales Risiko, Incident Response und Meldewege sollten dafür geübt sein. Quelle: https://www.oberberg-aktuell.de/blaulicht/stadtwerke-wurden-von-russischer-hackerbande-erpresst-a-139763	HOCH

ID	Meldung	Relevanz
L-02	UPDATE: Brotli-Lücke CVE-2026-111497 trifft Siemens Industrial Edge, für sieben Management-Apps gibt es noch keinen Fix (SSA-443410 vom 30.10.): Siemens nennt im Advisory CVSS v3.1 9,8 und CVSS v4.0 9,2. Die Industrial Edge Management Cloud ist laut Siemens seit 28.10. zentral gefixt, der Industrial Edge Hub seit 29.10., Anwender müssen dort nichts tun. Ohne Fix sind Cloud Connector Configurator, Common Configurator on Device (CC on Edge), Common Configurator (CC on IEM), Data Flow Monitoring, Databus Configurator, Edge OPC UA Server Configurator und Flow Creator Configurator. Siemens empfiehlt bis zum Fix, CC on Edge und Data Flow Monitoring zu stoppen; für die übrigen Apps alle Management Applications zu deinstallieren und die IEM-Instanz per Firewall/WAF zu schützen. Sind keine Management Applications installiert, ist laut Siemens nichts zu tun. Die CISA führt die Lücke in der Brotli-Bibliothek von Google seit 27.10. im KEV-Katalog, also als ausgenutzt (Frist für US-Behörden 10.11.). Für Betreiber, die Industrial Edge in Wasser- oder Energieanlagen einsetzen, heißt das: installierte Management-Apps prüfen und die Maßnahmen von Siemens umsetzen. Dieselbe Lücke betrifft laut SSA-898633 (30.10.) auch RUGGEDCOM APE1808 mit PAN-OS, eine Siemens-Plattform für Edge Computing und Cybersecurity in rauen Industrieumgebungen, auf der die Firewall-Software von Palo Alto Networks läuft. Siemens nennt dort keine konkrete Fix-Version und verweist auf das passende PAN-OS-Upgrade. Laut Palo Alto Networks betrifft die Lücke bei PAN-OS nur PA- und VM-Series-Firewalls, die Brotli-komprimierten Traffic prüfen und TLS/SSL-Decryption auf der Dataplane aktiv haben; die Management-Oberfläche (Web oder API) ist nicht betroffen. Gefixt ist PAN-OS ab 12.2.4-h1, 12.1.4-h13, 12.1.7-h11, 12.1.10-h3 sowie 11.2.4-h23, 11.2.7-h23, 11.2.10-h17, 11.2.13-h4 und 11.2.16-h1, PAN-OS 11.1 und 10.2 sind nicht betroffen. Als Workaround nennt Palo Alto Networks, die Brotli-Inspektion per CLI abzuschalten; ab PAN-OS 11.2.4 ist Brotli-Encoding standardmäßig aus. Eine Ausnutzung bei PAN-OS ist Palo Alto Networks laut eigenem Advisory nicht bekannt. Quellen: https://productcert.siemens.com/productcert/html/ssa-443410.html · https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json · https://productcert.siemens.com/productcert/html/ssa-898633.html · https://security.paloaltonetworks.com/CVE-2026-111497 (Erstmeldung am 28.10.2026: https://ot-cyber.de/ot-lage/2026-10-28.html)	HOCH
L-03	UK NCSC veröffentlicht „CAF Core Profile“ für kritische Infrastruktur (30.10.): Das Profil legt auf Basis des Cyber Assessment Framework v4.0 eine Mindest-Baseline für Organisationen fest, die „essential services“ erbringen oder kritische Infrastruktur unterstützen. Es richtet sich nach typischen Bedrohungen, das NCSC nennt unter anderem Ransomware und Angriffe über die Lieferkette. Eine Pflicht in DACH folgt daraus nicht, als Vergleichsmaßstab für NIS2- und KRITIS-Gespräche taugt es trotzdem. Quelle: https://www.ncsc.gov.uk/collection/cyber-assessment-framework/core-profile	MITTEL
L-04	Leak-Site-Einträge zu US-Energieunternehmen (26. bis 30.10., nicht bestätigt): Laut ransomware.live nennt DragonForce die Inside Passage Electric Cooperative (laut Breachsense ein Stromversorger in Südost-Alaska; entdeckt laut ransomware.live am 26.10., laut Breachsense am 27.10.), Qilin die Richland Resources Corporation und Akira FrenchCreek Production (beide entdeckt 30.10.). Das sind Behauptungen der Gruppen, Stellungnahmen der Unternehmen haben wir nicht gefunden. Einen direkten Bezug zu DACH gibt es nicht. Quellen: https://www.ransomware.live/activity/Energy%20&%20Utilities/US · https://www.breachsense.com/breaches/inside-passage-electric-cooperative-data-breach/	NIEDRIG

ID	Meldung	Relevanz
L-05	Ivanti Connect Secure: zwei ausgenutzte Lücken seit 30.10. im KEV-Katalog der CISA: Die CISA führt CVE-2026-111357 als „Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability“ und CVE-2026-118527 als „Ivanti Connect Secure Generation of Predictable Numbers or Identifiers Vulnerability“. Die Beschreibungen von CVE-2026-111357 weichen voneinander ab: Der KEV-Kasten bei SecurityOnline nennt für Version 22.8R2.4 einen Fehler im dsinvoked-Broker, der DSCache-Konfigurationsdaten vertraut (CVSS 7,0), der Artikeltext derselben Seite nennt fehlende Authentifizierung mit Rechteausweitung bis root und CVSS 8,8. CVE-2026-118527 betrifft laut SecurityOnline vorhersehbare Dateinamen: Ein angemeldeter Angreifer kann Schaddateien an bekannte Orte auf dem Gerät ablegen. Laut SecurityOnline nutzen Angreifer beide Lücken in einer Kette mit CVE-2026-104935 (Umgehung der Authentifizierung), um Root-Rechte zu bekommen. Das Ivanti-Advisory selbst konnten wir nicht prüfen. Für Betreiber, die Ivanti als VPN für die Fernwartung nutzen, heißt das: auf die Fix-Versionen aus dem Ivanti-Advisory aktualisieren (SecurityOnline nennt im Abschnitt zur Mitigation 25.1.1.3, 25.1.3.1 und 22.8R2.6, die Tabelle derselben Seite weicht davon ab), das Integrity Checker Tool von Ivanti laufen lassen, Logs prüfen und Zugangsdaten zurücksetzen, weil ein Patch bereits gestohlene Daten nicht ungültig macht. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://securityonline.info/ivanti-connect-secure-vulnerability-exploited/	HOCH
L-06	Nozomi Networks Guardian/CMC: Root-Codeausführung über Update-Pakete (NN-2026:21-01 und NN-2026:22-01, beide vom 29.10.): Betroffen sind Guardian und CMC vor Version 26.4.0. CVE-2026-33923 ist eine Umgehung der Signaturprüfung von Update-Paketen (CWE-347). Unter CVE-2026-33924 fasst Nozomi zwei OS Command Injections in der Update-Funktion zusammen (CWE-78). Beide haben CVSS v4 7,5. Ein Angreifer braucht Admin-Rechte und kann dann ein präpariertes Update-Paket einspielen, das als root läuft. Unsere Einschätzung: Betroffen sind damit die Sensoren zur Angriffserkennung (SzA) selbst, also die Systeme, die OT-Netze überwachen. Deshalb: auf 26.4.0 aktualisieren, Admin-Konten prüfen und die Weboberfläche per Firewall absichern. Quellen: https://security.nozominetworks.com/NN-2026:21-01 · https://security.nozominetworks.com/NN-2026:22-01	MITTEL
L-07	FortiBleed 2.0: weitere FortiGate-Konfigurationen mit Zugangsdaten im Umlauf: Laut The Hacker News (29.10.) hat Hudson Rock 1.703 Konfigurationsdateien von FortiGates mit insgesamt 40.573 Secrets ausgewertet, darunter 37.076 Datensätze lokaler Benutzerkonten und 1.576 LDAP-Bind-Datensätze fürs Active Directory. Das Material stammt laut Hudson Rock etwa aus dem Februar 2026. Die Zahlen kommen von Hudson Rock selbst, eine unabhängige Bestätigung haben wir nicht gefunden. Wer FortiGate am Übergang zwischen IT und OT betreibt, sollte VPN- und LDAP-Zugangsdaten wechseln, auch wenn die Firmware aktuell ist. Quellen: https://thehackernews.com/2026/10/threatsday-critical-firewall-flaws.html · https://www.infostealers.com/article/fortibleed-2-0-975-new-domains-40573-exposed-secrets-claim-your-ethical-disclosure/	MITTEL

ID	Meldung	Relevanz
L-08	Linux-Kernel: TCP-Lücke CVE-2026-98432, Kernel-CNA vergibt CVSS 9,8: Ursache ist ein Use-after-free bei der Verarbeitung von IPv4-TCP-Verbindungen, die Lücke steckt seit Kernel 4.4 im Code. Gemeldet hat sie ein Forscher von Anthropic. Der öffentlich gezeigte Root-Exploit setzt einen erreichbaren Multipath-TCP-Listener (MPTCP) voraus. Das Go-Security-Team schreibt aber, dass auch Systeme ohne MPTCP-Listener für ähnliche Angriffe anfällig sein könnten, und Go-Programme ab Version 1.24 öffnen MPTCP unter Linux standardmäßig. Die Bewertungen gehen auseinander: Red Hat, Amazon, Oracle und SUSE vergeben laut The Hacker News Werte zwischen 5,9 und 8,1. Angriffe in freier Wildbahn sind laut The Hacker News bisher nicht gemeldet. Ubuntu und RHEL hatten laut The Hacker News bis 29.10. noch keinen gefixten Kernel veröffentlicht, Debian, Oracle Linux (UEK) und Amazon Linux haben bereits gepatcht. Unsere Einschätzung: Betroffen sind vor allem Linux-basierte Gateways, Jump Hosts und SCADA-Server, auf denen Dienste mit MPTCP laufen: Kernel-Updates einplanen, Firmware-Hinweise der Hersteller verfolgen und bis dahin die von Red Hat beschriebene nftables-Regel prüfen. Quellen: https://thehackernews.com/2026/10/linux-kernel-tcp-flaw-with-98-cvss.html · https://access.redhat.com/security/vulnerabilities/RHSB-2026-016 · https://www.openwall.com/lists/oss-security/2026/10/30/1	MITTEL

Meldungen im Detail

L-01 Stadtwerke Waldbröl (NRW) erpresst, Kundendaten abgeflossen: Laut Oberberg-Aktuell vom 30.10. wurden die Stadtwerke rund drei Wochen vor dem Bericht erpresst, die Täter drohten mit der Veröffentlichung von Kundendaten. Geschäftsführer Mirco Kujbida spricht von einer „finanziell motivierten, russischen Hackerbande“. Das Unternehmen beauftragte IT-Forensiker, laut Unternehmen wurden tatsächlich Daten gestohlen. Wie viele Kunden betroffen sind, steht laut Bericht noch nicht fest. Versorgung und Erreichbarkeit waren laut Kujbida zu keinem Zeitpunkt unterbrochen oder gefährdet, die Sicherheitslücke ist laut Artikel behoben, das LKA ermittelt. Einen Gruppennamen und den Angriffsweg nennt der Bericht nicht. Wir haben dazu nur diese eine Quelle gefunden. Unsere Einschätzung: Auch ohne Eingriff in die Leittechnik bleibt für Stadtwerke die Erpressung mit Kundendaten ein reales Risiko, Incident Response und Meldewege sollten dafür geübt sein. Quelle: https://www.oberberg-aktuell.de/blaulicht/stadtwerke-wurden-von-russischer-hackerbande-erpresst-a-139763

Relevanz: HOCH

L-02 UPDATE: Brotli-Lücke CVE-2026-111497 trifft Siemens Industrial Edge, für sieben Management-Apps gibt es noch keinen Fix (SSA-443410 vom 30.10.): Siemens nennt im Advisory CVSS v3.1 9,8 und CVSS v4.0 9,2. Die Industrial Edge Management Cloud ist laut Siemens seit 28.10. zentral gefixt, der Industrial Edge Hub seit 29.10., Anwender müssen dort nichts tun. Ohne Fix sind Cloud Connector Configurator, Common Configurator on Device (CC on Edge), Common Configurator (CC on IEM), Data Flow Monitoring, Databus Configurator, Edge OPC UA Server Configurator und Flow Creator Configurator. Siemens empfiehlt bis zum Fix, CC on Edge und Data Flow Monitoring zu stoppen; für die übrigen Apps alle Management Applications zu deinstallieren und die IEM-Instanz per Firewall/WAF zu schützen. Sind keine Management Applications installiert, ist laut Siemens nichts zu tun. Die CISA führt die Lücke in der Brotli-Bibliothek von Google seit 27.10. im KEV-Katalog, also als ausgenutzt (Frist für US-Behörden 10.11.). Für Betreiber, die Industrial Edge in Wasser- oder Energieanlagen einsetzen, heißt das: installierte Management-Apps prüfen und die Maßnahmen von Siemens umsetzen. Dieselbe Lücke betrifft laut SSA-898633 (30.10.) auch RUGGEDCOM APE1808 mit PAN-OS, eine Siemens-Plattform für Edge Computing und Cybersecurity in rauen Industrieumgebungen, auf der die Firewall-Software von Palo Alto Networks läuft. Siemens nennt dort keine konkrete Fix-Version und verweist auf das passende PAN-OS-Upgrade. Laut Palo Alto Networks betrifft die Lücke bei PAN-OS nur PA- und VM-Series-Firewalls, die Brotli-komprimierten Traffic prüfen und TLS/SSL-Decryption auf der Dataplane aktiv haben; die Management-Oberfläche (Web oder API) ist nicht betroffen. Gefixt ist PAN-OS ab 12.2.4-h1, 12.1.4-h13, 12.1.7-h11, 12.1.10-h3 sowie 11.2.4-h23, 11.2.7-h23, 11.2.10-h17, 11.2.13-h4 und 11.2.16-h1, PAN-OS 11.1 und 10.2 sind nicht betroffen. Als Workaround nennt Palo Alto Networks, die Brotli-Inspektion per CLI abzuschalten; ab PAN-OS 11.2.4 ist Brotli-Encoding standardmäßig aus. Eine Ausnutzung bei PAN-OS ist Palo Alto Networks laut eigenem Advisory nicht bekannt. Quellen: https://productcert.siemens.com/productcert/html/ssa-443410.html · https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json · https://productcert.siemens.com/productcert/html/ssa-898633.html · https://security.paloaltonetworks.com/CVE-2026-111497 (Erstmeldung am 28.10.2026: https://ot-cyber.de/ot-lage/2026-10-28.html)

Relevanz: HOCH

L-03 UK NCSC veröffentlicht „CAF Core Profile“ für kritische Infrastruktur (30.10.): Das Profil legt auf Basis des Cyber Assessment Framework v4.0 eine Mindest-Baseline für Organisationen fest, die „essential services“ erbringen oder kritische Infrastruktur unterstützen. Es richtet sich nach typischen Bedrohungen, das NCSC nennt unter anderem Ransomware und Angriffe über die Lieferkette. Eine Pflicht in DACH folgt daraus nicht, als Vergleichsmaßstab für NIS2- und KRITIS-Gespräche taugt es trotzdem. Quelle: https://www.ncsc.gov.uk/collection/cyber-assessment-framework/core-profile

Relevanz: MITTEL

L-04 Leak-Site-Einträge zu US-Energieunternehmen (26. bis 30.10., nicht bestätigt): Laut ransomware.live nennt DragonForce die Inside Passage Electric Cooperative (laut Breachsense ein Stromversorger in Südost-Alaska; entdeckt laut ransomware.live am 26.10., laut Breachsense am 27.10.), Qilin die Richland Resources Corporation und Akira FrenchCreek Production (beide entdeckt 30.10.). Das sind Behauptungen der Gruppen, Stellungnahmen der Unternehmen haben wir nicht gefunden. Einen direkten Bezug zu DACH gibt es nicht. Quellen: https://www.ransomware.live/activity/Energy%20&%20Utilities/US · https://www.breachsense.com/breaches/inside-passage-electric-cooperative-data-breach/

Relevanz: NIEDRIG

L-05 Ivanti Connect Secure: zwei ausgenutzte Lücken seit 30.10. im KEV-Katalog der CISA: Die CISA führt CVE-2026-111357 als „Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability“ und CVE-2026-118527 als „Ivanti Connect Secure Generation of Predictable Numbers or Identifiers Vulnerability“. Die Beschreibungen von CVE-2026-111357 weichen voneinander ab: Der KEV-Kasten bei SecurityOnline nennt für Version 22.8R2.4 einen Fehler im dsinvoked-Broker, der DSCache-Konfigurationsdaten vertraut (CVSS 7,0), der Artikeltext derselben Seite nennt fehlende Authentifizierung mit Rechteausweitung bis root und CVSS 8,8. CVE-2026-118527 betrifft laut SecurityOnline vorhersehbare Dateinamen: Ein angemeldeter Angreifer kann Schaddateien an bekannte Orte auf dem Gerät ablegen. Laut SecurityOnline nutzen Angreifer beide Lücken in einer Kette mit CVE-2026-104935 (Umgehung der Authentifizierung), um Root-Rechte zu bekommen. Das Ivanti-Advisory selbst konnten wir nicht prüfen. Für Betreiber, die Ivanti als VPN für die Fernwartung nutzen, heißt das: auf die Fix-Versionen aus dem Ivanti-Advisory aktualisieren (SecurityOnline nennt im Abschnitt zur Mitigation 25.1.1.3, 25.1.3.1 und 22.8R2.6, die Tabelle derselben Seite weicht davon ab), das Integrity Checker Tool von Ivanti laufen lassen, Logs prüfen und Zugangsdaten zurücksetzen, weil ein Patch bereits gestohlene Daten nicht ungültig macht. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://securityonline.info/ivanti-connect-secure-vulnerability-exploited/

Relevanz: HOCH

L-06 Nozomi Networks Guardian/CMC: Root-Codeausführung über Update-Pakete (NN-2026:21-01 und NN-2026:22-01, beide vom 29.10.): Betroffen sind Guardian und CMC vor Version 26.4.0. CVE-2026-33923 ist eine Umgehung der Signaturprüfung von Update-Paketen (CWE-347). Unter CVE-2026-33924 fasst Nozomi zwei OS Command Injections in der Update-Funktion zusammen (CWE-78). Beide haben CVSS v4 7,5. Ein Angreifer braucht Admin-Rechte und kann dann ein präpariertes Update-Paket einspielen, das als root läuft. Unsere Einschätzung: Betroffen sind damit die Sensoren zur Angriffserkennung (SzA) selbst, also die Systeme, die OT-Netze überwachen. Deshalb: auf 26.4.0 aktualisieren, Admin-Konten prüfen und die Weboberfläche per Firewall absichern. Quellen: https://security.nozominetworks.com/NN-2026:21-01 · https://security.nozominetworks.com/NN-2026:22-01

Relevanz: MITTEL

L-07 FortiBleed 2.0: weitere FortiGate-Konfigurationen mit Zugangsdaten im Umlauf: Laut The Hacker News (29.10.) hat Hudson Rock 1.703 Konfigurationsdateien von FortiGates mit insgesamt 40.573 Secrets ausgewertet, darunter 37.076 Datensätze lokaler Benutzerkonten und 1.576 LDAP-Bind-Datensätze fürs Active Directory. Das Material stammt laut Hudson Rock etwa aus dem Februar 2026. Die Zahlen kommen von Hudson Rock selbst, eine unabhängige Bestätigung haben wir nicht gefunden. Wer FortiGate am Übergang zwischen IT und OT betreibt, sollte VPN- und LDAP-Zugangsdaten wechseln, auch wenn die Firmware aktuell ist. Quellen: https://thehackernews.com/2026/10/threatsday-critical-firewall-flaws.html · https://www.infostealers.com/article/fortibleed-2-0-975-new-domains-40573-exposed-secrets-claim-your-ethical-disclosure/

Relevanz: MITTEL

L-08 Linux-Kernel: TCP-Lücke CVE-2026-98432, Kernel-CNA vergibt CVSS 9,8: Ursache ist ein Use-after-free bei der Verarbeitung von IPv4-TCP-Verbindungen, die Lücke steckt seit Kernel 4.4 im Code. Gemeldet hat sie ein Forscher von Anthropic. Der öffentlich gezeigte Root-Exploit setzt einen erreichbaren Multipath-TCP-Listener (MPTCP) voraus. Das Go-Security-Team schreibt aber, dass auch Systeme ohne MPTCP-Listener für ähnliche Angriffe anfällig sein könnten, und Go-Programme ab Version 1.24 öffnen MPTCP unter Linux standardmäßig. Die Bewertungen gehen auseinander: Red Hat, Amazon, Oracle und SUSE vergeben laut The Hacker News Werte zwischen 5,9 und 8,1. Angriffe in freier Wildbahn sind laut The Hacker News bisher nicht gemeldet. Ubuntu und RHEL hatten laut The Hacker News bis 29.10. noch keinen gefixten Kernel veröffentlicht, Debian, Oracle Linux (UEK) und Amazon Linux haben bereits gepatcht. Unsere Einschätzung: Betroffen sind vor allem Linux-basierte Gateways, Jump Hosts und SCADA-Server, auf denen Dienste mit MPTCP laufen: Kernel-Updates einplanen, Firmware-Hinweise der Hersteller verfolgen und bis dahin die von Red Hat beschriebene nftables-Regel prüfen. Quellen: https://thehackernews.com/2026/10/linux-kernel-tcp-flaw-with-98-cvss.html · https://access.redhat.com/security/vulnerabilities/RHSB-2026-016 · https://www.openwall.com/lists/oss-security/2026/10/30/1

Relevanz: MITTEL

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