OT-CYBER.DE

LAGEBILD

# OT-/Cyber-Lagebild

Ausgabe 21.10.2026, 16:15 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

| | |
|---|---|
| **Zielgruppe** | Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS |
| **Datum** | 21.10.2026 |
| **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 12 Meldungen, davon 5 mit hoher Relevanz für Betreiber in DACH.

• Hitachi Energy RTU500: neues Advisory mit DoS-Lücke im IEC-104-Stack und acht weiteren CVEs (ICSA-26-293-05, 20.10.) Eigenes Advisory, nicht der schon gemeldete Firmware-Upload-Fall (CVE-2026-8065/-8066). Es geht um einen Denial of Service in der IEC 60870-5-104-Kommunikation (CVE-2026-17539) und um weitere Lücken, darunter eine Umgehung der Authentifizierung (CVE-2026-8932). Die höchste Bewertung liegt bei CVSS v3.1 8,8 (CVE-2026-6653). Betroffen ist die CMU-Firmware 12.7.1 bis 12.7.7 sowie 13.5.1 bis 13.8.2. Fix: 13.9.1 für alle Linien, alternativ 12.7.8 bzw. 13.8.3; 13.7.9 ist angekündigt. CISA nennt den Sektor Energie mit weltweitem Einsatz. Die CISA-Kopfzeile spricht von 7 Lücken, die Tabelle listet 9 CVEs. Fernwirk- und Netzbetreiber sollten das Asset-Inventar abgleichen und den Wechsel auf 13.9.1 einplanen (CC5 Risk-Based Vulnerability Management). Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-05

• Palo Alto PAN-OS GlobalProtect (CVE-2026-0257): Ransomware-Gruppen nutzen die Lücke, auch gegen Versorger Unit 42 hat seine Analyse am 19.10. ergänzt und nennt Qilin und Inc als Ransomware-Gruppen, die die Lücke ausnutzen wollen; Settra wird nur in öffentlichen Berichten genannt, Unit 42 bestätigt das nicht. Unter den betroffenen Branchen steht „utilities and energy“. Am 20.10. kam ein Hinweis dazu: GlobalProtect-Profile auf dem Management-Interface (Ports 4443 und 3879) können dieses Interface unbemerkt aus dem Internet erreichbar machen. Es ist nicht die schon gemeldete CVE-2026-0322. CVE-2026-0257 steht seit 13.05.2026 im KEV-Katalog (CC4 Secure Remote Access). Quelle: https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/

• BSI warnt vor kritischen PHP-Lücken (21.10.) Laut BSI sind alle bekannten PHP-Versionen bis mindestens PHP 5 verwundbar, Angreifer könnten Schadcode auf Webservern mit PHP-Anwendungen ausführen. Die Patches sollten am 21.10. um 16 Uhr deutscher Zeit erscheinen. Das BSI hält eine Ausnutzung in großem Stil innerhalb weniger Stunden für wahrscheinlich, weil KI-Werkzeuge Exploits schnell aus den Updates ableiten können. Die Pressemitteilung nennt keine CVE; Unit 42 führt die Lücken in seiner PAN-OS-Analyse (Link oben) als CVE-2026-109618 und CVE-2026-109619. Es ist eine IT-Lücke, sie betrifft aber auch Kundenportale, Störungsmelder und Webseiten von Versorgern: sofort patchen und den Patchstand prüfen. Quelle: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261021_PHP-kritische-Schwachstelle.html

• SafePay-Ransomware: gemeinsame Warnung von FBI, CISA, LKA Rheinland-Pfalz und britischen Behörden (AA26-293A, 20.10.) SafePay hat laut Advisory mindestens 600 Opfer, als Zielgruppe nennen die Behörden ausdrücklich auch OT-Betreiber. Initial Access läuft über Phishing, Brute Force, VPN-Konten und Edge Devices; genannt werden unter anderem CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711 und CVE-2024-40766. Für Betreiber in DACH ist das eine direkte Prüfliste für Remote Access und Backup-Server (CC4 Secure Remote Access). Quelle: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a

• Hitachi Energy MicroSCADA X SYS600: Anmeldung umgehbar, Adminrechte möglich (ICSA-26-293-04, 20.10.) Ein lokaler Nutzer kann die Anmeldung umgehen (CVE-2026-9853) und Windows-Adminrechte erlangen (CVE-2026-9854), dazu kommt eine CSV-Injection (CVE-2026-9852). Für Version 10.7 und älter hilft das Update auf 10.8, für CVE-2026-9854 in 10.8 gibt es noch keinen Fix. SYS600 steckt in vielen Netzleitstellen von Stadtwerken. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-04

**GESAMTBEWERTUNG**

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

# Lageübersicht

| ID | Meldung | Relevanz |
|---|---|---|
| L-01 | Hitachi Energy RTU500: neues Advisory mit DoS-Lücke im IEC-104-Stack und acht weiteren CVEs (ICSA-26-293-05, 20.10.) Eigenes Advisory, nicht der schon gemeldete Firmware-Upload-Fall (CVE-2026-8065/-8066). Es geht um einen Denial of Service in der IEC 60870-5-104-Kommunikation (CVE-2026-17539) und um weitere Lücken, darunter eine Umgehung der Authentifizierung (CVE-2026-8932). Die höchste Bewertung liegt bei CVSS v3.1 8,8 (CVE-2026-6653). Betroffen ist die CMU-Firmware 12.7.1 bis 12.7.7 sowie 13.5.1 bis 13.8.2. Fix: 13.9.1 für alle Linien, alternativ 12.7.8 bzw. 13.8.3; 13.7.9 ist angekündigt. CISA nennt den Sektor Energie mit weltweitem Einsatz. Die CISA-Kopfzeile spricht von 7 Lücken, die Tabelle listet 9 CVEs. Fernwirk- und Netzbetreiber sollten das Asset-Inventar abgleichen und den Wechsel auf 13.9.1 einplanen (CC5 Risk-Based Vulnerability Management). Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-05 | HOCH |
| L-02 | Palo Alto PAN-OS GlobalProtect (CVE-2026-0257): Ransomware-Gruppen nutzen die Lücke, auch gegen Versorger Unit 42 hat seine Analyse am 19.10. ergänzt und nennt Qilin und Inc als Ransomware-Gruppen, die die Lücke ausnutzen wollen; Settra wird nur in öffentlichen Berichten genannt, Unit 42 bestätigt das nicht. Unter den betroffenen Branchen steht „utilities and energy“. Am 20.10. kam ein Hinweis dazu: GlobalProtect-Profile auf dem Management-Interface (Ports 4443 und 3879) können dieses Interface unbemerkt aus dem Internet erreichbar machen. Es ist nicht die schon gemeldete CVE-2026-0322. CVE-2026-0257 steht seit 13.05.2026 im KEV-Katalog (CC4 Secure Remote Access). Quelle: https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/ | HOCH |
| L-03 | BSI warnt vor kritischen PHP-Lücken (21.10.) Laut BSI sind alle bekannten PHP-Versionen bis mindestens PHP 5 verwundbar, Angreifer könnten Schadcode auf Webservern mit PHP-Anwendungen ausführen. Die Patches sollten am 21.10. um 16 Uhr deutscher Zeit erscheinen. Das BSI hält eine Ausnutzung in großem Stil innerhalb weniger Stunden für wahrscheinlich, weil KI-Werkzeuge Exploits schnell aus den Updates ableiten können. Die Pressemitteilung nennt keine CVE; Unit 42 führt die Lücken in seiner PAN-OS-Analyse (Link oben) als CVE-2026-109618 und CVE-2026-109619. Es ist eine IT-Lücke, sie betrifft aber auch Kundenportale, Störungsmelder und Webseiten von Versorgern: sofort patchen und den Patchstand prüfen. Quelle: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261021_PHP-kritische-Schwachstelle.html | HOCH |
| L-04 | Accenture, Dragos und SANS: Stiftung mit rund 10 Mio. US-Dollar für kleine US-Versorger (20.10.) Die „Community Cyber Resilience Foundation“ unterstützt in der ersten Phase bis zu 500 US-Versorger für Wasser, Abwasser, Strom und Gas mit weniger als 100 Mio. US-Dollar Jahresumsatz. Sie bekommen kostenlos Security-Werkzeuge, Hardware, Hilfe bei der Einrichtung und Schulungen. Quelle: https://www.securityweek.com/accenture-dragos-sans-launch-10m-initiative-to-defend-small-us-utilities/ | MITTEL |

| ID | Meldung | Relevanz |
|---|---|---|
| L-05 | SafePay-Ransomware: gemeinsame Warnung von FBI, CISA, LKA Rheinland-Pfalz und britischen Behörden (AA26-293A, 20.10.) SafePay hat laut Advisory mindestens 600 Opfer, als Zielgruppe nennen die Behörden ausdrücklich auch OT-Betreiber. Initial Access läuft über Phishing, Brute Force, VPN-Konten und Edge Devices; genannt werden unter anderem CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711 und CVE-2024-40766. Für Betreiber in DACH ist das eine direkte Prüfliste für Remote Access und Backup-Server (CC4 Secure Remote Access). Quelle: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a | HOCH |
| L-06 | Hitachi Energy MicroSCADA X SYS600: Anmeldung umgehbar, Adminrechte möglich (ICSA-26-293-04, 20.10.) Ein lokaler Nutzer kann die Anmeldung umgehen (CVE-2026-9853) und Windows-Adminrechte erlangen (CVE-2026-9854), dazu kommt eine CSV-Injection (CVE-2026-9852). Für Version 10.7 und älter hilft das Update auf 10.8, für CVE-2026-9854 in 10.8 gibt es noch keinen Fix. SYS600 steckt in vielen Netzleitstellen von Stadtwerken. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-04 | HOCH |
| L-07 | UPDATE: Update Siemens Software Center (CVE-2026-110936): jetzt im KEV-Katalog (20.10.) CISA hat die Lücke in den Katalog aktiv ausgenutzter Schwachstellen aufgenommen. Die Ausnutzung über ClickFix-Köder ist damit offiziell bestätigt, Engineering-PCs mit Siemens-Software zuerst patchen. Quelle: https://www.cisa.gov/news-events/alerts/2026/10/20/cisa-adds-six-known-exploited-vulnerabilities-catalog (Erstmeldung am 20.10.2026: https://ot-cyber.de/ot-lage/2026-10-20.html) | MITTEL |
| L-08 | METTLER TOLEDO STARe: kritische Lücke in der mitgelieferten Datenbank (VDE-2026-112, 20.10.) Die eingebaute IBM-Db2-Komponente erlaubt Remote Code Execution ohne Anmeldung (CVE-2026-10109, CVSS 9,8). Abhilfe ist Db2 12.1.4 Update 87349. Betrifft Labore in Lebensmittel- und Chemieproduktion. Quelle: https://certvde.com/de/advisories/VDE-2026-112/ | MITTEL |
| L-09 | Moxa AIG-302 ThingsPro Edge: hartcodierter Schlüssel (ICSA-26-293-03, 20.10.) Bis Version 1.4.0 stecken ein hartcodierter Schlüssel (CVE-2026-109813, CVSS 8,1) und eine fehlende Berechtigungsprüfung (CVE-2026-109812) im Gateway, ausnutzbar aus dem lokalen Netz. Fix ist Firmware 1.4.1; CISA nennt Energie, Wasser/Abwasser und Fertigung. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-03 | MITTEL |
| L-10 | Festo CEPE mit AX OS: zwei OpenSSL-Lücken, Fix noch nicht verfügbar (VDE-2026-090, 20.10.) Betroffen sind CVE-2025-15467 (CVSS 9,8) und CVE-2025-69419. Der Fix AX OS 26.3.1.4 ist angekündigt; bis dahin den Zugriff auf die Steuerung aus dem Netz einschränken. Relevant für Maschinenbauer und deren Kunden. Quelle: https://certvde.com/de/advisories/VDE-2026-090/ | MITTEL |
| L-11 | Pilz IndustrialPI 4: Path Traversal und CSRF in PiCtory/RevPiPyLoad (VDE-2026-101, 20.10.) Neues Advisory PPSA-2026-005 (nicht das schon gemeldete PPSA-2026-004): Dateien lassen sich lesen oder löschen (CVE-2026-57472, CVE-2026-57471), die CSRF-Lücke (CVE-2026-57469) greift über den Browser eines Bedieners. Gefunden von Nozomi Networks Labs, Fix: PiCtory 2.17.0 und RevPiPyLoad 0.11.1. Quelle: https://certvde.com/de/advisories/VDE-2026-101/ | MITTEL |

| ID | Meldung | Relevanz |
|---|---|---|
| L-12 | PEAK-System PCAN-Treiber für Windows: sechs Lücken (ICSA-26-293-01, 20.10.) Bis Version 5.1.2 bringen lokal ausnutzbare Lücken (u. a. CVE-2026-103672) den Windows-Kernel zum Absturz. Fix ist 5.1.4. Betrifft Engineering- und Diagnose-PCs mit CAN-Bus im Maschinenbau. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-01 | MITTEL |

## Meldungen im Detail

### L-01 Hitachi Energy RTU500: neues Advisory mit DoS-Lücke im IEC-104-Stack und acht weiteren CVEs (ICSA-26-293-05, 20.10.) Eigenes Advisory, nicht der schon gemeldete Firmware-Upload-Fall (CVE-2026-8065/-8066). Es geht um einen Denial of Service in der IEC 60870-5-104-Kommunikation (CVE-2026-17539) und um weitere Lücken, darunter eine Umgehung der Authentifizierung (CVE-2026-8932). Die höchste Bewertung liegt bei CVSS v3.1 8,8 (CVE-2026-6653). Betroffen ist die CMU-Firmware 12.7.1 bis 12.7.7 sowie 13.5.1 bis 13.8.2. Fix: 13.9.1 für alle Linien, alternativ 12.7.8 bzw. 13.8.3; 13.7.9 ist angekündigt. CISA nennt den Sektor Energie mit weltweitem Einsatz. Die CISA-Kopfzeile spricht von 7 Lücken, die Tabelle listet 9 CVEs. Fernwirk- und Netzbetreiber sollten das Asset-Inventar abgleichen und den Wechsel auf 13.9.1 einplanen (CC5 Risk-Based Vulnerability Management). Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-05

Relevanz: HOCH

### L-02 Palo Alto PAN-OS GlobalProtect (CVE-2026-0257): Ransomware-Gruppen nutzen die Lücke, auch gegen Versorger Unit 42 hat seine Analyse am 19.10. ergänzt und nennt Qilin und Inc als Ransomware-Gruppen, die die Lücke ausnutzen wollen; Settra wird nur in öffentlichen Berichten genannt, Unit 42 bestätigt das nicht. Unter den betroffenen Branchen steht „utilities and energy“. Am 20.10. kam ein Hinweis dazu: GlobalProtect-Profile auf dem Management-Interface (Ports 4443 und 3879) können dieses Interface unbemerkt aus dem Internet erreichbar machen. Es ist nicht die schon gemeldete CVE-2026-0322. CVE-2026-0257 steht seit 13.05.2026 im KEV-Katalog (CC4 Secure Remote Access). Quelle: https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/

Relevanz: HOCH

**L-03 BSI warnt vor kritischen PHP-Lücken (21.10.) Laut BSI sind alle bekannten PHP-Versionen bis mindestens PHP 5 verwundbar, Angreifer könnten Schadcode auf Webservern mit PHP-Anwendungen ausführen. Die Patches sollten am 21.10. um 16 Uhr deutscher Zeit erscheinen. Das BSI hält eine Ausnutzung in großem Stil innerhalb weniger Stunden für wahrscheinlich, weil KI-Werkzeuge Exploits schnell aus den Updates ableiten können. Die Pressemitteilung nennt keine CVE; Unit 42 führt die Lücken in seiner PAN-OS-Analyse (Link oben) als CVE-2026-109618 und CVE-2026-109619. Es ist eine IT-Lücke, sie betrifft aber auch Kundenportale, Störungsmelder und Webseiten von Versorgern: sofort patchen und den Patchstand prüfen. Quelle: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261021_PHP-kritische-Schwachstelle.html**

Relevanz: HOCH

**L-04 Accenture, Dragos und SANS: Stiftung mit rund 10 Mio. US-Dollar für kleine US-Versorger (20.10.) Die „Community Cyber Resilience Foundation“ unterstützt in der ersten Phase bis zu 500 US-Versorger für Wasser, Abwasser, Strom und Gas mit weniger als 100 Mio. US-Dollar Jahresumsatz. Sie bekommen kostenlos Security-Werkzeuge, Hardware, Hilfe bei der Einrichtung und Schulungen. Quelle: https://www.securityweek.com/accenture-dragos-sans-launch-10m-initiative-to-defend-small-us-utilities/**

Relevanz: MITTEL

**L-05 SafePay-Ransomware: gemeinsame Warnung von FBI, CISA, LKA Rheinland-Pfalz und britischen Behörden (AA26-293A, 20.10.) SafePay hat laut Advisory mindestens 600 Opfer, als Zielgruppe nennen die Behörden ausdrücklich auch OT-Betreiber. Initial Access läuft über Phishing, Brute Force, VPN-Konten und Edge Devices; genannt werden unter anderem CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711 und CVE-2024-40766. Für Betreiber in DACH ist das eine direkte Prüfliste für Remote Access und Backup-Server (CC4 Secure Remote Access). Quelle: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a**

Relevanz: HOCH

**L-06 Hitachi Energy MicroSCADA X SYS600: Anmeldung umgehbar, Adminrechte möglich (ICSA-26-293-04, 20.10.) Ein lokaler Nutzer kann die Anmeldung umgehen (CVE-2026-9853) und Windows-Adminrechte erlangen (CVE-2026-9854), dazu kommt eine CSV-Injection (CVE-2026-9852). Für Version 10.7 und älter hilft das Update auf 10.8, für CVE-2026-9854 in 10.8 gibt es noch keinen Fix. SYS600 steckt in vielen Netzleitstellen von Stadtwerken. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-04**

Relevanz: HOCH

**L-07 □ UPDATE: Update Siemens Software Center (CVE-2026-110936): jetzt im KEV-Katalog (20.10.) CISA hat die Lücke in den Katalog aktiv ausgenutzter Schwachstellen aufgenommen. Die Ausnutzung über ClickFix-Köder ist damit offiziell bestätigt, Engineering-PCs mit Siemens-Software zuerst patchen. Quelle: https://www.cisa.gov/news-events/alerts/2026/10/20/cisa-adds-six-known-exploited-vulnerabilities-catalog (Erstmeldung am 20.10.2026: https://ot-cyber.de/ot-lage/2026-10-20.html)**

Relevanz: MITTEL

**L-08 METTLER TOLEDO STARe: kritische Lücke in der mitgelieferten Datenbank (VDE-2026-112, 20.10.) Die eingebaute IBM-Db2-Komponente erlaubt Remote Code Execution ohne Anmeldung (CVE-2026-10109, CVSS 9,8). Abhilfe ist Db2 12.1.4 Update 87349. Betrifft Labore in Lebensmittel- und Chemieproduktion. Quelle: https://certvde.com/de/advisories/VDE-2026-112/**

Relevanz: MITTEL

**L-09 Moxa AIG-302 ThingsPro Edge: hartcodierter Schlüssel (ICSA-26-293-03, 20.10.) Bis Version 1.4.0 stecken ein hartcodierter Schlüssel (CVE-2026-109813, CVSS 8,1) und eine fehlende Berechtigungsprüfung (CVE-2026-109812) im Gateway, ausnutzbar aus dem lokalen Netz. Fix ist Firmware 1.4.1; CISA nennt Energie, Wasser/Abwasser und Fertigung. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-03**

Relevanz: MITTEL

**L-10 Festo CEPE mit AX OS: zwei OpenSSL-Lücken, Fix noch nicht verfügbar (VDE-2026-090, 20.10.) Betroffen sind CVE-2025-15467 (CVSS 9,8) und CVE-2025-69419. Der Fix AX OS 26.3.1.4 ist angekündigt; bis dahin den Zugriff auf die Steuerung aus dem Netz einschränken. Relevant für Maschinenbauer und deren Kunden. Quelle: https://certvde.com/de/advisories/VDE-2026-090/**

Relevanz: MITTEL

**L-11 Pilz IndustrialPI 4: Path Traversal und CSRF in PiCtory/RevPiPyLoad (VDE-2026-101, 20.10.) Neues Advisory PPSA-2026-005 (nicht das schon gemeldete PPSA-2026-004): Dateien lassen sich lesen oder löschen (CVE-2026-57472, CVE-2026-57471), die CSRF-Lücke (CVE-2026-57469) greift über den Browser eines Bedieners. Gefunden von Nozomi Networks Labs, Fix: PiCtory 2.17.0 und RevPiPyLoad 0.11.1. Quelle: https://certvde.com/de/advisories/VDE-2026-101/**

Relevanz: MITTEL

### L-12 PEAK-System PCAN-Treiber für Windows: sechs Lücken (ICSA-26-293-01, 20.10.) Bis Version 5.1.2 bringen lokal ausnutzbare Lücken (u. a. CVE-2026-103672) den Windows-Kernel zum Absturz. Fix ist 5.1.4. Betrifft Engineering- und Diagnose-PCs mit CAN-Bus im Maschinenbau. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-01

Relevanz: MITTEL

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