OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 27.10.2026, 07:28 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	27.10.2026
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 4 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• UPDATE: PHP2Shell seit 26.10. im KEV-Katalog, OT-Hersteller melden betroffene Produkte (Stand 27.10.): Die CISA hat am 26.10. CVE-2026-109618 („PHP Memory Corruption“) und CVE-2026-109619 („Stale Internal Request-State“) in den KEV-Katalog aufgenommen. Damit gelten beide Lücken offiziell als aktiv ausgenutzt. Palo Alto schreibt dagegen in seinem Advisory (aktualisiert am 27.10.), dass dem Hersteller keine Ausnutzung gegen eigene Produkte bekannt ist. Für PAN-OS stehen erste Hotfixes bereit (zum Beispiel 12.2.4-h1, 11.2.10-h16, 10.2.18-h13), weitere sind für 27. bis 30.10. angekündigt. Bei Siemens gibt es inzwischen zwei Advisories: In SSA-566512 (23.10.) ist RUGGEDCOM APE1808 mit PAN-OS 10.2 bis 12.2 als betroffen bestätigt, einen Patch gibt es nur über den Siemens-Support. Das neue SSA-166980 (26.10.) betrifft Gebäude-, Zutritts- und Videotechnik: Dort stehen 15 Produkte als „nicht betroffen“, weil sie kein PHP enthalten, darunter Desigo CC, Desigo PXC4/PXC5/PXC7, Climatix, Connect X200/X300/X500, SiPass integrated und Siveillance Video. Siemens prüft weiter und weist darauf hin, dass sich die Einstufung noch ändern kann. Für Fernwartung und Leittechnik in DACH sind drei weitere Herstellermeldungen wichtig. Belden (PSIRT-10, 22.10.): Alle Versionen der NetModule Router Software (NRSW) sind betroffen, auch 5.0.0.104, einen Patch gibt es noch nicht. Belden empfiehlt, die Weboberfläche per SSH abzuschalten, bis ein Update erscheint. B&R (SA26P015, 23.10.): APROL bis R 4.4-65 ist betroffen. Patches hatte B&R im Advisory vom 23.10. für den 26.10. und den 29.10. angekündigt, bis zur Installation empfiehlt der Hersteller, HTTP(S)-Zugriffe auf das APROL-System an der Firewall zu sperren. HMS (HMSSAR-2026-10-22-001): eWON Flexy und Cosy+ sind nicht betroffen, die Talk2M-Dienste hat HMS am 21.10. gepatcht und keine Hinweise auf eine Kompromittierung gefunden. Unsere Empfehlung: Wer NetModule-Router oder APROL im Feld hat, klärt heute, von wo die Weboberfläche erreichbar ist, und lässt sie bis zum Patch nur aus dem Management-Netz zu. Zuerst kommen die Geräte mit erreichbarer Weboberfläche dran, danach der Rest (Risk-Based Vulnerability Management, der fünfte der SANS Five ICS Cybersecurity Critical Controls). Quellen: https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://security.paloaltonetworks.com/CVE-2026-109618 · https://cert-portal.siemens.com/productcert/html/ssa-566512.html · https://cert-portal.siemens.com/productcert/html/ssa-166980.html · https://assets.belden.com/asset/0e20ea6c-c1f5-4269-b765-e160a2bf4965/PSIRT-10-Critical-PHP-Vulnerabilities-in-macmon-and-NRSW.pdf · https://br-cws-assets.de-fra-1.linodeobjects.com/SA26P015-7cd6ca9c.pdf · https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/cybersecurity/security-advisory/hms-security-advisory-2026-10-22-001---talk2m--ewon-flexy-and-cosy-php-vulnerabilities.pdf (Erstmeldung am 24.10.2026: https://ot-cyber.de/ot-lage/2026-10-24.html)

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	UPDATE: PHP2Shell seit 26.10. im KEV-Katalog, OT-Hersteller melden betroffene Produkte (Stand 27.10.): Die CISA hat am 26.10. CVE-2026-109618 („PHP Memory Corruption“) und CVE-2026-109619 („Stale Internal Request-State“) in den KEV-Katalog aufgenommen. Damit gelten beide Lücken offiziell als aktiv ausgenutzt. Palo Alto schreibt dagegen in seinem Advisory (aktualisiert am 27.10.), dass dem Hersteller keine Ausnutzung gegen eigene Produkte bekannt ist. Für PAN-OS stehen erste Hotfixes bereit (zum Beispiel 12.2.4-h1, 11.2.10-h16, 10.2.18-h13), weitere sind für 27. bis 30.10. angekündigt. Bei Siemens gibt es inzwischen zwei Advisories: In SSA-566512 (23.10.) ist RUGGEDCOM APE1808 mit PAN-OS 10.2 bis 12.2 als betroffen bestätigt, einen Patch gibt es nur über den Siemens-Support. Das neue SSA-166980 (26.10.) betrifft Gebäude-, Zutritts- und Videotechnik: Dort stehen 15 Produkte als „nicht betroffen“, weil sie kein PHP enthalten, darunter Desigo CC, Desigo PXC4/PXC5/PXC7, Climatix, Connect X200/X300/X500, SiPass integrated und Siveillance Video. Siemens prüft weiter und weist darauf hin, dass sich die Einstufung noch ändern kann. Für Fernwartung und Leittechnik in DACH sind drei weitere Herstellermeldungen wichtig. Belden (PSIRT-10, 22.10.): Alle Versionen der NetModule Router Software (NRSW) sind betroffen, auch 5.0.0.104, einen Patch gibt es noch nicht. Belden empfiehlt, die Weboberfläche per SSH abzuschalten, bis ein Update erscheint. B&R (SA26P015, 23.10.): APROL bis R 4.4-65 ist betroffen. Patches hatte B&R im Advisory vom 23.10. für den 26.10. und den 29.10. angekündigt, bis zur Installation empfiehlt der Hersteller, HTTP(S)-Zugriffe auf das APROL-System an der Firewall zu sperren. HMS (HMSSAR-2026-10-22-001): eWON Flexy und Cosy+ sind nicht betroffen, die Talk2M-Dienste hat HMS am 21.10. gepatcht und keine Hinweise auf eine Kompromittierung gefunden. Unsere Empfehlung: Wer NetModule-Router oder APROL im Feld hat, klärt heute, von wo die Weboberfläche erreichbar ist, und lässt sie bis zum Patch nur aus dem Management-Netz zu. Zuerst kommen die Geräte mit erreichbarer Weboberfläche dran, danach der Rest (Risk-Based Vulnerability Management, der fünfte der SANS Five ICS Cybersecurity Critical Controls). Quellen: https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://security.paloaltonetworks.com/CVE-2026-109618 · https://cert-portal.siemens.com/productcert/html/ssa-566512.html · https://cert-portal.siemens.com/productcert/html/ssa-166980.html · https://assets.belden.com/asset/0e20ea6c-c1f5-4269-b765-e160a2bf4965/PSIRT-10-Critical-PHP-Vulnerabilities-in-macmon-and-NRSW.pdf · https://br-cws-assets.de-fra-1.linodeobjects.com/SA26P015-7cd6ca9c.pdf · https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/cybersecurity/security-advisory/hms-security-advisory-2026-10-22-001---talk2m--ewon-flexy-and-cosy-php-vulnerabilities.pdf (Erstmeldung am 24.10.2026: https://ot-cyber.de/ot-lage/2026-10-24.html)	HOCH
L-02	Qilin nennt den US-Stromversorger Delta Electric Power Association als Opfer (26.10.): Die Ransomware-Gruppe Qilin führt die Delta Electric Power Association (Sektor Energie und Versorgung, USA) seit dem 26.10. auf ihrer Leak-Seite. Das ist bisher nur die Behauptung der Angreifer. Eine Stellungnahme des Versorgers, Angaben zum Ausmaß oder Hinweise auf eine Beteiligung der OT haben wir nicht gefunden. Quelle: https://www.ransomware.live/id/RGVsdGEgRWxlY3RyaWMgUG93ZXIgQXNzb2NpYXRpb25AcWlsaW4	MITTEL

ID	Meldung	Relevanz
L-03	CERT-UA: Angreifer übernehmen Dahua-Überwachungskameras und Rekorder (Bericht vom 26.10.): Laut CERT-UA haben Angreifer Dahua-Kameras und -NVRs mit Internetzugang übernommen. Mutmaßlicher Weg ist die Cloud-Fernzugriffsfunktion Easy4IP, deren Seriennummern vorhersehbaren Mustern folgen. Danach probieren die Angreifer schwache oder Standardpasswörter oder nutzen alte Lücken wie CVE-2021-33044 und CVE-2021-33045. Wer dahintersteckt, ist offen. Laut Hunt.io können bösartige Konten und Recovery-Codes einen Passwortwechsel überleben, auf den meisten Firmware-Ständen auch einen Werksreset. Konten zu löschen reicht ohne Firmware-Update nicht. Die Meldung betrifft die Ukraine, Versorger werden nicht genannt. Wer Dahua-Kameras an Pumpwerken, Hochbehältern oder Umspannwerken betreibt, sollte trotzdem prüfen, ob Easy4IP aktiv ist, die Firmware aktualisieren und die Kameras vom Prozessnetz trennen. Quelle: https://therecord.media/ukraine-cert-ua-warning-chinese-dahua-cameras-hacked	MITTEL
L-04	Siemens Mendix: Authentication Bypass im SAML-Modul (SSA-137528, 26.10.): Ein Angreifer ohne Anmeldung kann eine gültige SAML-Antwort erneut einspielen (Replay) und sich so Zugang verschaffen (CVE-2026-89209, CVSS v3.1 6,8, v4.0 7,6). Betroffen ist das Mendix-SAML-Modul vor V3.6.29 (Mendix 9) und vor V4.2.4 (Mendix 10 und 11). Updates gibt es im Mendix Marketplace, bis dahin hilft es, das IdP-initiierte SSO abzuschalten. Das betrifft Betreiber, die eigene Mendix-Apps etwa für Instandhaltung oder Netzdaten mit SSO nutzen. Quelle: https://cert-portal.siemens.com/productcert/html/ssa-137528.html	MITTEL

Meldungen im Detail

L-01 UPDATE: PHP2Shell seit 26.10. im KEV-Katalog, OT-Hersteller melden betroffene Produkte (Stand 27.10.): Die CISA hat am 26.10. CVE-2026-109618 („PHP Memory Corruption“) und CVE-2026-109619 („Stale Internal Request-State“) in den KEV-Katalog aufgenommen. Damit gelten beide Lücken offiziell als aktiv ausgenutzt. Palo Alto schreibt dagegen in seinem Advisory (aktualisiert am 27.10.), dass dem Hersteller keine Ausnutzung gegen eigene Produkte bekannt ist. Für PAN-OS stehen erste Hotfixes bereit (zum Beispiel 12.2.4-h1, 11.2.10-h16, 10.2.18-h13), weitere sind für 27. bis 30.10. angekündigt. Bei Siemens gibt es inzwischen zwei Advisories: In SSA-566512 (23.10.) ist RUGGEDCOM APE1808 mit PAN-OS 10.2 bis 12.2 als betroffen bestätigt, einen Patch gibt es nur über den Siemens-Support. Das neue SSA-166980 (26.10.) betrifft Gebäude-, Zutritts- und Videotechnik: Dort stehen 15 Produkte als „nicht betroffen“, weil sie kein PHP enthalten, darunter Desigo CC, Desigo PXC4/PXC5/PXC7, Climatix, Connect X200/X300/X500, SiPass integrated und Siveillance Video. Siemens prüft weiter und weist darauf hin, dass sich die Einstufung noch ändern kann. Für Fernwartung und Leittechnik in DACH sind drei weitere Herstellermeldungen wichtig. Belden (PSIRT-10, 22.10.): Alle Versionen der NetModule Router Software (NRSW) sind betroffen, auch 5.0.0.104, einen Patch gibt es noch nicht. Belden empfiehlt, die Weboberfläche per SSH abzuschalten, bis ein Update erscheint. B&R (SA26P015, 23.10.): APROL bis R 4.4-65 ist betroffen. Patches hatte B&R im Advisory vom 23.10. für den 26.10. und den 29.10. angekündigt, bis zur Installation empfiehlt der Hersteller, HTTP(S)-Zugriffe auf das APROL-System an der Firewall zu sperren. HMS (HMSSAR-2026-10-22-001): eWON Flexy und Cosy+ sind nicht betroffen, die Talk2M-Dienste hat HMS am 21.10. gepatcht und keine Hinweise auf eine Kompromittierung gefunden. Unsere Empfehlung: Wer NetModule-Router oder APROL im Feld hat, klärt heute, von wo die Weboberfläche erreichbar ist, und lässt sie bis zum Patch nur aus dem Management-Netz zu. Zuerst kommen die Geräte mit erreichbarer Weboberfläche dran, danach der Rest (Risk-Based Vulnerability Management, der fünfte der SANS Five ICS Cybersecurity Critical Controls). Quellen: https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://security.paloaltonetworks.com/CVE-2026-109618 · https://cert-portal.siemens.com/productcert/html/ssa-566512.html · https://cert-portal.siemens.com/productcert/html/ssa-166980.html · https://assets.belden.com/asset/0e20ea6c-c1f5-4269-b765-e160a2bf4965/PSIRT-10-Critical-PHP-Vulnerabilities-in-macmon-and-NRSW.pdf · https://br-cws-assets.de-fra-1.linodeobjects.com/SA26P015-7cd6ca9c.pdf · https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/cybersecurity/security-advisory/hms-security-advisory-2026-10-22-001---talk2m--ewon-flexy-and-cosy-php-vulnerabilities.pdf (Erstmeldung am 24.10.2026: https://ot-cyber.de/ot-lage/2026-10-24.html)

Relevanz: HOCH

L-02 Qilin nennt den US-Stromversorger Delta Electric Power Association als Opfer (26.10.): Die Ransomware-Gruppe Qilin führt die Delta Electric Power Association (Sektor Energie und Versorgung, USA) seit dem 26.10. auf ihrer Leak-Seite. Das ist bisher nur die Behauptung der Angreifer. Eine Stellungnahme des Versorgers, Angaben zum Ausmaß oder Hinweise auf eine Beteiligung der OT haben wir nicht gefunden. Quelle: https://www.ransomware.live/id/RGVsdGEgRWxlY3RyaWMgUG93ZXIgQXNzb2NpYXRpb25AcWlsaW4

Relevanz: MITTEL

L-03 CERT-UA: Angreifer übernehmen Dahua-Überwachungskameras und Rekorder (Bericht vom 26.10.): Laut CERT-UA haben Angreifer Dahua-Kameras und -NVRs mit Internetzugang übernommen. Mutmaßlicher Weg ist die Cloud-Fernzugriffsfunktion Easy4IP, deren Seriennummern vorhersehbaren Mustern folgen. Danach probieren die Angreifer schwache oder Standardpasswörter oder nutzen alte Lücken wie CVE-2021-33044 und CVE-2021-33045. Wer dahintersteckt, ist offen. Laut Hunt.io können bösartige Konten und Recovery-Codes einen Passwortwechsel überleben, auf den meisten Firmware-Ständen auch einen Werksreset. Konten zu löschen reicht ohne Firmware-Update nicht. Die Meldung betrifft die Ukraine, Versorger werden nicht genannt. Wer Dahua-Kameras an Pumpwerken, Hochbehältern oder Umspannwerken betreibt, sollte trotzdem prüfen, ob Easy4IP aktiv ist, die Firmware aktualisieren und die Kameras vom Prozessnetz trennen. Quelle: https://therecord.media/ukraine-cert-ua-warning-chinese-dahua-cameras-hacked

Relevanz: MITTEL

L-04 Siemens Mendix: Authentication Bypass im SAML-Modul (SSA-137528, 26.10.): Ein Angreifer ohne Anmeldung kann eine gültige SAML-Antwort erneut einspielen (Replay) und sich so Zugang verschaffen (CVE-2026-89209, CVSS v3.1 6,8, v4.0 7,6). Betroffen ist das Mendix-SAML-Modul vor V3.6.29 (Mendix 9) und vor V4.2.4 (Mendix 10 und 11). Updates gibt es im Mendix Marketplace, bis dahin hilft es, das IdP-initiierte SSO abzuschalten. Das betrifft Betreiber, die eigene Mendix-Apps etwa für Instandhaltung oder Netzdaten mit SSO nutzen. Quelle: https://cert-portal.siemens.com/productcert/html/ssa-137528.html

Relevanz: MITTEL

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