

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 30.10.2026, 16:17 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	30.10.2026
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 5 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

- Sophos UTM: Root-Codeausführung ohne Anmeldung (CVE-2026-118633, 28.10.): Laut Sophos-Advisory vom 28.10. betrifft die Path-Traversal-Lücke alle Versionen von Sophos UTM (laut CVE-Eintrag bis einschließlich 9.724), wenn der E-Mail-Proxy mit aktiviertem Scanning (Email Protection) läuft. Ein Angreifer ohne Zugangsdaten kann aus der Ferne Befehle als root ausführen, muss dafür aber über einige Minuten eine Race Condition gewinnen. Einen Workaround gibt es nicht. UTM ist seit dem 30.06.2026 End of Life, nach dem 31.12.2026 gibt es laut Sophos gar keinen Support mehr. Sophos nennt zwei Wege: den manuellen Patch nach KBA-000049692 oder den Umstieg auf Sophos Firewall. Laut Brandefense muss die UTM dafür zuerst auf 9.724 aktualisiert werden, danach folgt der RPM-Patch (die KBA-Seite selbst konnten wir nicht abrufen). Zur Ausnutzung macht Sophos keine Angaben, im KEV-Katalog der CISA steht die Lücke nicht. Sophos selbst stuft sie als kritisch ein, der CVE-Eintrag nennt CVSS 8.1 (Version 3.1) bzw. 9.2 (Version 4.0). CERT-Bund führt sie als WID-SEC-W-2026-4232 mit Risiko hoch. Unsere Einschätzung: Bei Stadtwerken und Industriebetrieben in DACH kommen alte UTMs als Mail-Gateway oder an der Grenze zwischen IT und OT vor. Wer Email Protection nutzt, sollte heute patchen und den Umstieg einplanen. Quellen:

<https://www.sophos.com/en-us/security-advisories/sophos-sa-20261028-utm-rce> ·

<https://cveawg.mitre.org/api/cve/CVE-2026-118633> ·

<https://wid.cert-bund.de/.well-known/csaf/white/2026/wid-sec-w-2026-4232.json> · <https://brandefense.io/security-news/sophos-utm-cve-2026-118633-email-protection-rce-patch/> · <https://community.sophos.com/utm-firewall/lifecycle-and-migration/f/recommended-reads/139151/sophos-utm-sg-end-of-life-frequently-asked-questions>

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	<p>Sophos UTM: Root-Codeausführung ohne Anmeldung (CVE-2026-118633, 28.10.): Laut Sophos-Advisory vom 28.10. betrifft die Path-Traversal-Lücke alle Versionen von Sophos UTM (laut CVE-Eintrag bis einschließlich 9.724), wenn der E-Mail-Proxy mit aktiviertem Scanning (Email Protection) läuft. Ein Angreifer ohne Zugangsdaten kann aus der Ferne Befehle als root ausführen, muss dafür aber über einige Minuten eine Race Condition gewinnen. Einen Workaround gibt es nicht. UTM ist seit dem 30.06.2026 End of Life, nach dem 31.12.2026 gibt es laut Sophos gar keinen Support mehr. Sophos nennt zwei Wege: den manuellen Patch nach KBA-000049692 oder den Umstieg auf Sophos Firewall. Laut Brandefense muss die UTM dafür zuerst auf 9.724 aktualisiert werden, danach folgt der RPM-Patch (die KBA-Seite selbst konnten wir nicht abrufen). Zur Ausnutzung macht Sophos keine Angaben, im KEV-Katalog der CISA steht die Lücke nicht. Sophos selbst stuft sie als kritisch ein, der CVE-Eintrag nennt CVSS 8.1 (Version 3.1) bzw. 9.2 (Version 4.0). CERT-Bund führt sie als WID-SEC-W-2026-4232 mit Risiko hoch. Unsere Einschätzung: Bei Stadtwerken und Industriebetrieben in DACH kommen alte UTMs als Mail-Gateway oder an der Grenze zwischen IT und OT vor. Wer Email Protection nutzt, sollte heute patchen und den Umstieg einplanen. Quellen: https://www.sophos.com/en-us/security-advisories/sophos-sa-20261028-utm-rce · https://cveawg.mitre.org/api/cve/CVE-2026-118633 · https://wid.cert-bund.de/.well-known/csaf/white/2026/wid-sec-w-2026-4232.json · https://brandefense.io/security-news/sophos-utm-cve-2026-118633-email-protection-rce-patch/ · https://community.sophos.com/utm-firewall/lifecycle-and-migration/f/recommended-reads/139151/sophos-utm-sg-end-of-life-frequently-asked-questions</p>	HOCH
L-02	<p>Juniper Session Smart Router und Conductor: 18 Lücken, darunter CVSS 9.8 (28.10.): Das kanadische Cyber Centre (AV26-1101, 28.10.) und CERT-Bund (WID-SEC-W-2026-4234, Risiko hoch) bestätigen das Juniper-Bulletin JSA112183. Betroffen sind Router und Conductor vor den Versionen 7.0.5, 7.1.7 und 7.2.3. CERT-Bund listet 18 CVEs. CVE-2026-103409 (CVSS 9.8) ist eine fehlende Authentifizierung an einem Endpunkt, der als root läuft. Ausnutzbar ist sie laut CVE-Eintrag nur, solange das Gerät noch nicht in Mist oder den Conductor eingebunden ist. CVE-2026-103408 (CVSS 8.8) ist ein Stack-Pufferüberlauf im DHCP-Client: Ein Angreifer im angrenzenden Netz kann ihn ohne Anmeldung mit einer manipulierten DHCP-Antwort auslösen, mit hohen Folgen für Vertraulichkeit, Integrität und Verfügbarkeit. Laut Juniper ist keine Ausnutzung bekannt, Workarounds gibt es nicht. Unsere Einschätzung: Versorger, die SSR als SD-WAN-Router für Außenstationen nutzen, sollten neue Geräte nur eingebunden in Betrieb nehmen und die Updates zeitnah einspielen. Quellen: https://cyber.gc.ca/en/alerts-advisories/juniper-networks-security-advisory-av26-1101 · https://wid.cert-bund.de/.well-known/csaf/white/2026/wid-sec-w-2026-4234.json · https://cveawg.mitre.org/api/cve/CVE-2026-103408 · https://cveawg.mitre.org/api/cve/CVE-2026-103409 · https://supportportal.juniper.net/JSA112183</p>	MITTEL

ID	Meldung	Relevanz
L-03	<p>Update: GitLab CVE-2026-97229 und Cisco ASA/FTD CVE-2026-76418 seit 29.10. im KEV-Katalog der CISA: Die CISA hat beide Lücken am 29.10. „based on evidence of active exploitation“ in den Katalog aufgenommen, also weil Belege für eine aktive Ausnutzung vorliegen. CVE-2026-97229 ist ein Integer Overflow in GitLab Community und Enterprise Edition, CVE-2026-76418 eine NULL-Pointer-Dereferenzierung in Cisco Secure Firewall ASA und Secure FTD. Für GitLab ist das gegenüber dem bestehenden Lagebild neu. Wer GitLab selbst betreibt, etwa für SPS- oder Konfigurations-Repos, und wer Cisco-Firewalls am Übergang von IT zu OT einsetzt, sollte das Patchen jetzt vorziehen. Quelle: https://www.cisa.gov/news-events/alerts/2026/10/29/cisa-adds-two-known-exploited-vulnerabilities-catalog</p>	MITTEL
L-04	<p>Bloomberg: Russland-nahe Hacktivist*innen verursachen physische Schäden an Wasser- und Industrieanlagen (27.10.): Bloomberg beschreibt, wie prorussische Gruppen schlecht gesicherte Steuerungen in Europa und den USA manipulieren. Physische Folgen nennt der Bericht unter anderem für die Wasseranlage im dänischen Tureby (Mitte Dezember 2024): Rund 450 Haushalte waren zunächst ohne Wasser. Nachdem der Betreiber den Druck wiederhergestellt hatte, stieg er am folgenden Morgen unkontrolliert an, und unterirdische Leitungen platzten. Zu diesem Angriff bekannte sich die Gruppe Z-Pentest. Der dänische Verteidigungsnachrichtendienst machte die Gruppe im Dezember 2025 dafür verantwortlich und ordnete sie dem russischen Staat zu (Euronews, 19.12.2025). Bei einem Fleischbetrieb nahe Los Angeles fiel die Kühlung aus, über 900 kg Fleisch verdarben, und wegen austretenden Ammoniaks wurde evakuiert. Als weitere betroffene Einrichtungen nennen die Berichte ein Wassersystem in Texas und eine Abwasserbehandlungsanlage in Pennsylvania (Oktober 2024), an der Geräte zur Abtötung von Bakterien manipuliert wurden. Die Gruppe Cyber Army of Russia Reborn (CARR) wurde laut US-Justizministerium mit Unterstützung des russischen Militärgeheimdienstes GRU aufgebaut und von ihm gelenkt. Ein Betreiber in DACH wird nicht genannt. Unsere Einschätzung: Die genannten Fälle stammen aus den Jahren 2024 bis 2026, neu ist vor allem die Zusammenschau. Für Wasser- und Abwasserbetriebe heißt das aus unserer Sicht: HMIs und Steuerungen, die offen im Internet erreichbar sind, gehören hinter einen abgesicherten Remote Access und ins Asset-Inventar. Quellen: https://www.bloomberg.com/news/features/2026-10-27/russia-linked-hackers-are-turning-cyberattacks-into-a-physical-threat · https://winfuture.de/news,162257.html · https://meduza.io/en/feature/2026/10/28/russia-linked-hackers-are-exploiting-poorly-secured-industrial-systems-to-sabotage-factories-utilities-and-food-production-across-the-west-bloom</p>	MITTEL

ID	Meldung	Relevanz
L-05	<p>Japan: Einbruch in das Meldeportal der Strom- und Gasmarktaufsicht: Die Electricity and Gas Market Surveillance Commission des japanischen Wirtschaftsministeriums METI hat am 28.10. bekanntgegeben, dass Unbekannte in den frühen Morgenstunden des 27.10. unbefugt auf ihr Meldeportal „Dentori-Net“ zugegriffen haben. Über das Portal reichen Strom- und Gasversorger ihre regelmäßigen Berichte ein, etwa zu Absatzmengen. Die Kommission hat die Seite abgeschaltet und nimmt Berichte bis zur Wiederherstellung per E-Mail an. Ob Daten abgefließen sind, wird noch geprüft, laut Niigata Nippo könnten Finanzdaten der Unternehmen betroffen sein. Angaben zu Tätern oder Vorgehen gibt es nicht. Für die Daseinsvorsorge in DACH zeigt das: Auch die Meldeportale von Behörden und Marktplätzen sind Angriffsfläche, über die Geschäftsdaten von Versorgern abfließen können. Quellen: https://news.web.nhk/newsweb/na/nd-20261028dw67403 · https://www.sbbit.jp/article/cont1/187889 · https://www.niigata-nippo.co.jp/articles/-/932948</p>	MITTEL

Meldungen im Detail

L-01 Sophos UTM: Root-Codeausführung ohne Anmeldung (CVE-2026-118633, 28.10.): Laut Sophos-Advisory vom 28.10. betrifft die Path-Traversal-Lücke alle Versionen von Sophos UTM (laut CVE-Eintrag bis einschließlich 9.724), wenn der E-Mail-Proxy mit aktiviertem Scanning (Email Protection) läuft. Ein Angreifer ohne Zugangsdaten kann aus der Ferne Befehle als root ausführen, muss dafür aber über einige Minuten eine Race Condition gewinnen. Einen Workaround gibt es nicht. UTM ist seit dem 30.06.2026 End of Life, nach dem 31.12.2026 gibt es laut Sophos gar keinen Support mehr. Sophos nennt zwei Wege: den manuellen Patch nach KBA-000049692 oder den Umstieg auf Sophos Firewall. Laut Brandefense muss die UTM dafür zuerst auf 9.724 aktualisiert werden, danach folgt der RPM-Patch (die KBA-Seite selbst konnten wir nicht abrufen). Zur Ausnutzung macht Sophos keine Angaben, im KEV-Katalog der CISA steht die Lücke nicht. Sophos selbst stuft sie als kritisch ein, der CVE-Eintrag nennt CVSS 8.1 (Version 3.1) bzw. 9.2 (Version 4.0). CERT-Bund führt sie als WID-SEC-W-2026-4232 mit Risiko hoch. Unsere Einschätzung: Bei Stadtwerken und Industriebetrieben in DACH kommen alte UTMs als Mail-Gateway oder an der Grenze zwischen IT und OT vor. Wer Email Protection nutzt, sollte heute patchen und den Umstieg einplanen. Quellen: <https://www.sophos.com/en-us/security-advisories/sophos-sa-20261028-utm-rce> · <https://cveawg.mitre.org/api/cve/CVE-2026-118633> · <https://wid.cert-bund.de/.well-known/csaf/white/2026/wid-sec-w-2026-4232.json> · <https://brandefense.io/security-news/sophos-utm-cve-2026-118633-email-protection-rce-patch/> · <https://community.sophos.com/utm-firewall/lifecycle-and-migration/f/recommended-reads/139151/sophos-utm-sg-end-of-life-frequently-asked-questions>

Relevanz: **HOCH**

L-02 Juniper Session Smart Router und Conductor: 18 Lücken, darunter CVSS 9.8 (28.10.): Das kanadische Cyber Centre (AV26-1101, 28.10.) und CERT-Bund (WID-SEC-W-2026-4234, Risiko hoch) bestätigen das Juniper-Bulletin JSA112183. Betroffen sind Router und Conductor vor den Versionen 7.0.5, 7.1.7 und 7.2.3. CERT-Bund listet 18 CVEs. CVE-2026-103409 (CVSS 9.8) ist eine fehlende Authentifizierung an einem Endpunkt, der als root läuft. Ausnutzbar ist sie laut CVE-Eintrag nur, solange das Gerät noch nicht in Mist oder den Conductor eingebunden ist. CVE-2026-103408 (CVSS 8.8) ist ein Stack-Pufferüberlauf im DHCP-Client: Ein Angreifer im angrenzenden Netz kann ihn ohne Anmeldung mit einer manipulierten DHCP-Antwort auslösen, mit hohen Folgen für Vertraulichkeit, Integrität und Verfügbarkeit. Laut Juniper ist keine Ausnutzung bekannt, Workarounds gibt es nicht. Unsere Einschätzung: Versorger, die SSR als SD-WAN-Router für Außenstationen nutzen, sollten neue Geräte nur eingebunden in Betrieb nehmen und die Updates zeitnah einspielen. Quellen: <https://cyber.gc.ca/en/alerts-advisories/juniper-networks-security-advisory-av26-1101> · <https://wid.cert-bund.de/.well-known/csaf/white/2026/wid-sec-w-2026-4234.json> · <https://cveawg.mitre.org/api/cve/CVE-2026-103408> · <https://cveawg.mitre.org/api/cve/CVE-2026-103409> · <https://supportportal.juniper.net/JSA112183>

Relevanz: MITTEL

L-03 Update: GitLab CVE-2026-97229 und Cisco ASA/FTD CVE-2026-76418 seit 29.10. im KEV-Katalog der CISA: Die CISA hat beide Lücken am 29.10. „based on evidence of active exploitation“ in den Katalog aufgenommen, also weil Belege für eine aktive Ausnutzung vorliegen. CVE-2026-97229 ist ein Integer Overflow in GitLab Community und Enterprise Edition, CVE-2026-76418 eine NULL-Pointer-Dereferenzierung in Cisco Secure Firewall ASA und Secure FTD. Für GitLab ist das gegenüber dem bestehenden Lagebild neu. Wer GitLab selbst betreibt, etwa für SPS- oder Konfigurations-Repos, und wer Cisco-Firewalls am Übergang von IT zu OT einsetzt, sollte das Patchen jetzt vorziehen. Quelle: <https://www.cisa.gov/news-events/alerts/2026/10/29/cisa-adds-two-known-exploited-vulnerabilities-catalog>

Relevanz: MITTEL

L-04 Bloomberg: Russland-nahe Hacktivisten verursachen physische Schäden an Wasser- und Industrieanlagen (27.10.): Bloomberg beschreibt, wie prorussische Gruppen schlecht gesicherte Steuerungen in Europa und den USA manipulieren. Physische Folgen nennt der Bericht unter anderem für die Wasseranlage im dänischen Tureby (Mitte Dezember 2024): Rund 450 Haushalte waren zunächst ohne Wasser. Nachdem der Betreiber den Druck wiederhergestellt hatte, stieg er am folgenden Morgen unkontrolliert an, und unterirdische Leitungen platzten. Zu diesem Angriff bekannte sich die Gruppe Z-Pentest. Der dänische Verteidigungsnachrichtendienst machte die Gruppe im Dezember 2025 dafür verantwortlich und ordnete sie dem russischen Staat zu (Euronews, 19.12.2025). Bei einem Fleischbetrieb nahe Los Angeles fiel die Kühlung aus, über 900 kg Fleisch verdarben, und wegen austretenden Ammoniaks wurde evakuiert. Als weitere betroffene Einrichtungen nennen die Berichte ein Wassersystem in Texas und eine Abwasserbehandlungsanlage in Pennsylvania (Oktober 2024), an der Geräte zur Abtötung von Bakterien manipuliert wurden. Die Gruppe Cyber Army of Russia Reborn (CARR) wurde laut US-Justizministerium mit Unterstützung des russischen Militäргеheimdienstes GRU aufgebaut und von ihm gelenkt. Ein Betreiber in DACH wird nicht genannt. Unsere Einschätzung: Die genannten Fälle stammen aus den Jahren 2024 bis 2026, neu ist vor allem die Zusammenschau. Für Wasser- und Abwasserbetriebe heißt das aus unserer Sicht: HMIs und Steuerungen, die offen im Internet erreichbar sind, gehören hinter einen abgesicherten Remote Access und ins Asset-Inventar. Quellen: <https://www.bloomberg.com/news/features/2026-10-27/russia-linked-hackers-are-turning-cyberattacks-into-a-physical-threat> · <https://winfuture.de/news,162257.html> · <https://meduza.io/en/feature/2026/10/28/russia-linked-hackers-are-exploiting-poorly-secured-industrial-systems-to-sabotage-factories-utilities-and-food-production-across-the-west-bloom>

Relevanz: MITTEL

L-05 Japan: Einbruch in das Meldeportal der Strom- und Gasmarktaufsicht: Die Electricity and Gas Market Surveillance Commission des japanischen Wirtschaftsministeriums METI hat am 28.10. bekanntgegeben, dass Unbekannte in den frühen Morgenstunden des 27.10. unbefugt auf ihr Meldeportal „Dentori-Net“ zugegriffen haben. Über das Portal reichen Strom- und Gasversorger ihre regelmäßigen Berichte ein, etwa zu Absatzmengen. Die Kommission hat die Seite abgeschaltet und nimmt Berichte bis zur Wiederherstellung per E-Mail an. Ob Daten abgeflossen sind, wird noch geprüft, laut Niigata Nippo könnten Finanzdaten der Unternehmen betroffen sein. Angaben zu Tätern oder Vorgehen gibt es nicht. Für die Daseinsvorsorge in DACH zeigt das: Auch die Meldeportale von Behörden und Marktplätzen sind Angriffsfläche, über die Geschäftsdaten von Versorgern abfließen können. Quellen: <https://news.web.nhk/newsweb/na/nd-20261028dw67403> · <https://www.sbbit.jp/article/cont1/187889> · <https://www.niigata-nippo.co.jp/articles/-/932948>

Relevanz: MITTEL

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