OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 17.10.2026, 09:43 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	17.10.2026
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 3 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• **BeyondTrust Remote Support: Zero-Day wird aktiv ausgenutzt (CVE-2026-102764, KEV seit 16.10.)**: Über die Lücke können Angreifer die Anmeldung umgehen und beliebige Dateien hochladen. Betroffen sind alle Versionen bis 26.2.3, der Patch heißt BT26-05-RS. Laut Mandiant hat die mutmaßlich China-nahe Gruppe ARMORY CASTLE (früher als UNC5221 geführt) die Lücke bereits Ende August 2026 als Zero-Day ausgenutzt, laut CISA wird sie aktiv ausgenutzt. Die Gruppe legt dabei die Webshell SAWFLY ab. Selbst gehostete Appliances brauchen den Patch BT26-05-RS, die SaaS-Variante ist laut CISA bereits gepatcht. Bei Versionen vor 24.3.1 ist zuerst ein Upgrade nötig. Unsere Einschätzung: Wo BeyondTrust Remote Support (früher Bomgar) als Fernwartungs-Zugang für Dienstleister dient, sollten Betreiber prüfen, ob er bis in die Leittechnik reicht. Ebenso unsere Einschätzung: Erreichbare, selbst betriebene Appliances sollten bis zur Prüfung als kompromittiert behandelt werden, denn der Patch entfernt keine Angreifer, die schon drin sind. Deshalb patchen und auf Kompromittierung prüfen. CISA nennt nur „critical“ und keine CVSS-Zahl. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-urges-patching-critical-vulnerability-beyondtrust-remote-support · https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust · https://labs.beazley.security/advisories/BSL-A1231

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**BeyondTrust Remote Support: Zero-Day wird aktiv ausgenutzt (CVE-2026-102764, KEV seit 16.10.)**: Über die Lücke können Angreifer die Anmeldung umgehen und beliebige Dateien hochladen. Betroffen sind alle Versionen bis 26.2.3, der Patch heißt BT26-05-RS. Laut Mandiant hat die mutmaßlich China-nahe Gruppe ARMORY CASTLE (früher als UNC5221 geführt) die Lücke bereits Ende August 2026 als Zero-Day ausgenutzt, laut CISA wird sie aktiv ausgenutzt. Die Gruppe legt dabei die Webshell SAWFLY ab. Selbst gehostete Appliances brauchen den Patch BT26-05-RS, die SaaS-Variante ist laut CISA bereits gepatcht. Bei Versionen vor 24.3.1 ist zuerst ein Upgrade nötig. Unsere Einschätzung: Wo BeyondTrust Remote Support (früher Bomgar) als Fernwartungs-Zugang für Dienstleister dient, sollten Betreiber prüfen, ob er bis in die Leittechnik reicht. Ebenso unsere Einschätzung: Erreichbare, selbst betriebene Appliances sollten bis zur Prüfung als kompromittiert behandelt werden, denn der Patch entfernt keine Angreifer, die schon drin sind. Deshalb patchen und auf Kompromittierung prüfen. CISA nennt nur „critical“ und keine CVSS-Zahl. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-urges-patching-critical-vulnerability-beyondtrust-remote-support · https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust · https://labs.beazley.security/advisories/BSL-A1231	HOCH

ID	Meldung	Relevanz
L-02	**Fortinet FortiOS, FortiProxy, FortiPAM und FortiSwitchManager: Path Traversal in der Kommandozeile jetzt im KEV-Katalog (CVE-2025-61624, KEV seit 16.10.)**: Über die Lücke im Kommandozeilen-Interpreter kann ein angemeldeter Admin mit Schreibrechten beliebige Dateien schreiben oder löschen. Ein Patch liegt vor, laut CISA wird die Lücke jetzt ausgenutzt. Unsere Einschätzung: Weil Admin-Rechte nötig sind, wird die Lücke wahrscheinlich mit einer anderen kombiniert. FortiGate wird auch als Firewall zwischen IT und OT eingesetzt. Deshalb Versionen prüfen und Admin-Zugänge zur Management-Oberfläche einschränken. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://www.wiz.io/de-de/vulnerability-database/cve/cve-2025-61624	MITTEL
L-03	**Forschung „ICS-Sniper“: Angriff auf Cloud-SCADA trotz verschlüsseltem VPN (University of British Columbia)**: Forschende der University of British Columbia zeigen einen Proof of Concept. Wer einen Router auf dem Weg zwischen Anlage und Cloud-Leitstand kontrolliert, erkennt wichtige Steuerbefehle allein an Größe und Timing der verschlüsselten VPN-Pakete und kann sie gezielt verwerfen. Im Test an einer nachgebauten Wasseraufbereitung ließen sich so Abläufe wie Pumpen und Ventilsteuerung stören. Das ist ein Laborergebnis, kein echter Vorfall. Für Versorger mit Cloud-Fernwirktechnik heißt es aber: Verschlüsselung allein reicht nicht. Das Leitsystem muss ausbleibende Befehle und Antworten erkennen, und kritische Befehle brauchen einen Ersatzweg. Die erste Preprint-Fassung stammt von Dezember 2023, neu ist die überarbeitete Fassung. Quellen: https://www.securityweek.com/in-other-news-ics-sniper-attack-hacking-xworm-malware-operators-250k-chrome-exploit/ · https://techxplore.com/news/2026-10-cyber-threat-exposes-limits-encryption.html · https://arxiv.org/abs/2312.06140	MITTEL

Meldungen im Detail

L-01 **BeyondTrust Remote Support: Zero-Day wird aktiv ausgenutzt (CVE-2026-102764, KEV seit 16.10.): Über die Lücke können Angreifer die Anmeldung umgehen und beliebige Dateien hochladen. Betroffen sind alle Versionen bis 26.2.3, der Patch heißt BT26-05-RS. Laut Mandiant hat die mutmaßlich China-nahe Gruppe ARMORY CASTLE (früher als UNC5221 geführt) die Lücke bereits Ende August 2026 als Zero-Day ausgenutzt, laut CISA wird sie aktiv ausgenutzt. Die Gruppe legt dabei die Webshell SAWFLY ab. Selbst gehostete Appliances brauchen den Patch BT26-05-RS, die SaaS-Variante ist laut CISA bereits gepatcht. Bei Versionen vor 24.3.1 ist zuerst ein Upgrade nötig. Unsere Einschätzung: Wo BeyondTrust Remote Support (früher Bomgar) als Fernwartungs-Zugang für Dienstleister dient, sollten Betreiber prüfen, ob er bis in die Leittechnik reicht. Ebenso unsere Einschätzung: Erreichbare, selbst betriebene Appliances sollten bis zur Prüfung als kompromittiert behandelt werden, denn der Patch entfernt keine Angreifer, die schon drin sind. Deshalb patchen und auf Kompromittierung prüfen. CISA nennt nur „critical“ und keine CVSS-Zahl. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-urges-patching-critical-vulnerability-beyondtrust-remote-support · https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust · https://labs.beazley.security/advisories/BSL-A1231**

Relevanz: HOCH

L-02 **Fortinet FortiOS, FortiProxy, FortiPAM und FortiSwitchManager: Path Traversal in der Kommandozeile jetzt im KEV-Katalog (CVE-2025-61624, KEV seit 16.10.): Über die Lücke im Kommandozeilen-Interpreter kann ein angemeldeter Admin mit Schreibrechten beliebige Dateien schreiben oder löschen. Ein Patch liegt vor, laut CISA wird die Lücke jetzt ausgenutzt. Unsere Einschätzung: Weil Admin-Rechte nötig sind, wird die Lücke wahrscheinlich mit einer anderen kombiniert. FortiGate wird auch als Firewall zwischen IT und OT eingesetzt. Deshalb Versionen prüfen und Admin-Zugänge zur Management-Oberfläche einschränken. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://www.wiz.io/de-de/vulnerability-database/cve/cve-2025-61624**

Relevanz: MITTEL

L-03 **Forschung „ICS-Sniper“: Angriff auf Cloud-SCADA trotz verschlüsseltem VPN (University of British Columbia): Forschende der University of British Columbia zeigen einen Proof of Concept. Wer einen Router auf dem Weg zwischen Anlage und Cloud-Leitstand kontrolliert, erkennt wichtige Steuerbefehle allein an Größe und Timing der verschlüsselten VPN-Pakete und kann sie gezielt verwerfen. Im Test an einer nachgebauten Wasseraufbereitung ließen sich so Abläufe wie Pumpen und Ventilsteuerung stören. Das ist ein Laborergebnis, kein echter Vorfall. Für Versorger mit Cloud-Fernwirktechnik heißt es aber: Verschlüsselung allein reicht nicht. Das Leitsystem muss ausbleibende Befehle und Antworten erkennen, und kritische Befehle brauchen einen Ersatzweg. Die erste Preprint-Fassung stammt von Dezember 2023, neu ist die überarbeitete Fassung. Quellen: https://www.securityweek.com/in-other-news-ics-sniper-attack-hacking-xworm-malware-operators-250k-chrome-exploit/ · https://techxplore.com/news/2026-10-cyber-threat-exposes-limits-encryption.html · https://arxiv.org/abs/2312.06140**

Relevanz: MITTEL

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