

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 28.10.2026, 07:34 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	28.10.2026
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.

- Mitsubishi Electric ICONICS GENESIS64/GENESIS und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02, CISA 27.10.): Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, die für alle Benutzer gleich ist. Damit lässt sich das System aus der Ferne entsperren (CVE-2026-16436, CVSS v4 9,2). Am schwersten wiegt nach CVSS die Rechteauserweiterung CVE-2026-16438 (unnötige DCOM-Berechtigungen, CVSS v3.1 9,1, v4 9,4). Dazu kommen die lokale Lücke CVE-2026-16437 (CVSS v4 7,1) und die alte libwebp-Lücke CVE-2023-4863. Fixes gibt es mit GENESIS 11.04 und GENESIS64/Hyper Historian/AnalytiX/MobileHMI/IoTWorX 10.98. Für MC Works64, GENESIS32 und BizViz plant Mitsubishi keinen Fix und empfiehlt den Umstieg auf GENESIS64 bzw. GENESIS. Mitsubishi Electric empfiehlt außerdem, dass sich an den PCs mit dem betroffenen Produkt nur Administratoren anmelden dürfen. Unsere Einschätzung: GENESIS64/ICONICS kommt als SCADA/HMI und Historian auch in Wasser-, Energie- und Gebäudeleittechnik vor. Altinstallationen sollten deshalb ins Asset-Inventar und vom Remote Access getrennt werden. Laut Mitsubishi ist keine Ausnutzung bekannt. Das Mitsubishi-PSIRT-Advisory 2026-006 stammt bereits vom 15.10., CISA hat es am 27.10. veröffentlicht. Quellen: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02> · https://www.mitsubishielectric.com/psirt/vulnerability/pdf/2026-006_en.pdf

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Mitsubishi Electric ICONICS GENESIS64/GENESIS und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02, CISA 27.10.): Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, die für alle Benutzer gleich ist. Damit lässt sich das System aus der Ferne entsperren (CVE-2026-16436, CVSS v4 9,2). Am schwersten wiegt nach CVSS die Rechteauserweiterung CVE-2026-16438 (unnötige DCOM-Berechtigungen, CVSS v3.1 9,1, v4 9,4). Dazu kommen die lokale Lücke CVE-2026-16437 (CVSS v4 7,1) und die alte libwebp-Lücke CVE-2023-4863. Fixes gibt es mit GENESIS 11.04 und GENESIS64/Hyper Historian/AnalytiX/MobileHMI/IoTWorX 10.98. Für MC Works64, GENESIS32 und BizViz plant Mitsubishi keinen Fix und empfiehlt den Umstieg auf GENESIS64 bzw. GENESIS. Mitsubishi Electric empfiehlt außerdem, dass sich an den PCs mit dem betroffenen Produkt nur Administratoren anmelden dürfen. Unsere Einschätzung: GENESIS64/ICONICS kommt als SCADA/HMI und Historian auch in Wasser-, Energie- und Gebäudeleittechnik vor. Altinstallationen sollten deshalb ins Asset-Inventar und vom Remote Access getrennt werden. Laut Mitsubishi ist keine Ausnutzung bekannt. Das Mitsubishi-PSIRT-Advisory 2026-006 stammt bereits vom 15.10., CISA hat es am 27.10. veröffentlicht. Quellen: https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02 · https://www.mitsubishielectric.com/psirt/vulnerability/pdf/2026-006_en.pdf	HOCH

ID	Meldung	Relevanz
L-02	<p>Google-Brotli-Lücke (Node.js u. a.) seit 27.10. im KEV-Katalog der CISA (CVE-2026-111497): Der Brotli-Decoder hat laut Google und Node.js einen Out-of-Bounds-Write, der Remote Code Execution ermöglicht (CVSS v4 9,2). CISA führt die Lücke als „Google Brotli Unchecked Return Value Vulnerability“, Frist für US-Bundesbehörden ist der 10.11.2026. Betroffen sind laut Node.js-Security-Release vom 21.10. die Linien 22.x, 24.x und 26.x, dazu Bun, Python-Pakete und PHP für Windows. Fixes: Brotli 1.0.10, 1.1.1 und 1.2.1 (alle 21.10.) sowie Node.js 22.23.4, 24.22.1 und 26.12.1; die Distributionen liefern Backports nach. Mit der KEV-Aufnahme bestätigt die CISA die Ausnutzung. Für Versorger betrifft das Edge-Geräte, Gateways und Dashboards auf Node.js-Basis, zum Beispiel mit Node-RED. Ein Advisory von Node-RED oder einem OT-Hersteller gibt es bisher nicht, die Betroffenheit dort ist also abgeleitet. Ebenfalls am 27.10. kam Adobe Commerce/Magento (CVE-2026-48356) in den KEV-Katalog, ohne OT-Bezug. Quellen: https://www.cisa.gov/news-events/alerts/2026/10/27/cisa-adds-two-known-exploited-vulnerabilities-catalog · https://nodejs.org/en/blog/vulnerability/october-2026-security-releases · https://github.com/google/brotli/releases · https://www.tenable.com/blog/brotli2shell-frequently-asked-questions-for-google-brotli-decoder-cve-2026-111497</p>	MITTEL
L-03	<p>EPICS Base: kritischer Integer Overflow im Netzwerkprotokoll (ICSA-26-300-01, CISA 27.10.): Betroffen ist EPICS Base 7.0.10 und älter mit vier Lücken. Die schwerste, CVE-2026-114595 (CVSS v3.1 9,8, v4 9,3, Integer Overflow), kann ohne Anmeldung zu Speicherkorruption und möglicherweise zur Codeausführung führen. Dazu kommen CVE-2026-114596 (CVSS v3.1 8,2) sowie CVE-2026-114597 und CVE-2026-114598 (je 7,5). Fix: Version 7.0.11. Laut CISA ist keine Ausnutzung bekannt. Unsere Einschätzung: EPICS steuert vor allem Forschungsanlagen wie Beschleuniger und Teleskope, Stadtwerke und Wasserversorger dürften kaum direkt betroffen sein. Wer Forschungs- oder Großanlagen betreibt oder beliefert, sollte trotzdem kurz prüfen. Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-01</p>	MITTEL

Meldungen im Detail

L-01 Mitsubishi Electric ICONICS GENESIS64/GENESIS und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02, CISA 27.10.): Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, die für alle Benutzer gleich ist. Damit lässt sich das System aus der Ferne entsperren (CVE-2026-16436, CVSS v4 9,2). Am schwersten wiegt nach CVSS die Rechteauserweiterung CVE-2026-16438 (unnötige DCOM-Berechtigungen, CVSS v3.1 9,1, v4 9,4). Dazu kommen die lokale Lücke CVE-2026-16437 (CVSS v4 7,1) und die alte libwebp-Lücke CVE-2023-4863. Fixes gibt es mit GENESIS 11.04 und GENESIS64/Hyper Historian/AnalytiX/MobileHMI/loTWorkX 10.98. Für MC Works64, GENESIS32 und BizViz plant Mitsubishi keinen Fix und empfiehlt den Umstieg auf GENESIS64 bzw. GENESIS. Mitsubishi Electric empfiehlt außerdem, dass sich an den PCs mit dem betroffenen Produkt nur Administratoren anmelden dürfen. Unsere Einschätzung: GENESIS64/ICONICS kommt als SCADA/HMI und Historian auch in Wasser-, Energie- und Gebäudeleittechnik vor. Altinstallationen sollten deshalb ins Asset-Inventar und vom Remote Access getrennt werden. Laut Mitsubishi ist keine Ausnutzung bekannt. Das Mitsubishi-PSIRT-Advisory 2026-006 stammt bereits vom 15.10., CISA hat es am 27.10. veröffentlicht. Quellen: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02> · https://www.mitsubishielectric.com/psirt/vulnerability/pdf/2026-006_en.pdf

Relevanz: **HOCH**

L-02 Google-Brotli-Lücke (Node.js u. a.) seit 27.10. im KEV-Katalog der CISA (CVE-2026-111497): Der Brotli-Decoder hat laut Google und Node.js einen Out-of-Bounds-Write, der Remote Code Execution ermöglicht (CVSS v4 9,2). CISA führt die Lücke als „Google Brotli Unchecked Return Value Vulnerability“, Frist für US-Bundesbehörden ist der 10.11.2026. Betroffen sind laut Node.js-Security-Release vom 21.10. die Linien 22.x, 24.x und 26.x, dazu Bun, Python-Pakete und PHP für Windows. Fixes: Brotli 1.0.10, 1.1.1 und 1.2.1 (alle 21.10.) sowie Node.js 22.23.4, 24.22.1 und 26.12.1; die Distributionen liefern Backports nach. Mit der KEV-Aufnahme bestätigt die CISA die Ausnutzung. Für Versorger betrifft das Edge-Geräte, Gateways und Dashboards auf Node.js-Basis, zum Beispiel mit Node-RED. Ein Advisory von Node-RED oder einem OT-Hersteller gibt es bisher nicht, die Betroffenheit dort ist also abgeleitet. Ebenfalls am 27.10. kam Adobe Commerce/Magento (CVE-2026-48356) in den KEV-Katalog, ohne OT-Bezug. Quellen: <https://www.cisa.gov/news-events/alerts/2026/10/27/cisa-adds-two-known-exploited-vulnerabilities-catalog> · <https://nodejs.org/en/blog/vulnerability/october-2026-security-releases> · <https://github.com/google/brotli/releases> · <https://www.tenable.com/blog/brotli2shell-frequently-asked-questions-for-google-brotli-decoder-cve-2026-111497>

Relevanz: **MITTEL**

L-03 EPICS Base: kritischer Integer Overflow im Netzwerkprotokoll (ICSA-26-300-01, CISA 27.10.): Betroffen ist EPICS Base 7.0.10 und älter mit vier Lücken. Die schwerste, CVE-2026-114595 (CVSS v3.1 9,8, v4 9,3, Integer Overflow), kann ohne Anmeldung zu Speicherkorruption und möglicherweise zur Codeausführung führen. Dazu kommen CVE-2026-114596 (CVSS v3.1 8,2) sowie CVE-2026-114597 und CVE-2026-114598 (je 7,5). Fix: Version 7.0.11. Laut CISA ist keine Ausnutzung bekannt. Unsere Einschätzung: EPICS steuert vor allem Forschungsanlagen wie Beschleuniger und Teleskope, Stadtwerke und Wasserversorger dürften kaum direkt betroffen sein. Wer Forschungs- oder Großanlagen betreibt oder beliefert, sollte trotzdem kurz prüfen. Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-01>

Relevanz: MITTEL

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