

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 07.10.2026, 16:10 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	07.10.2026
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 11 Meldungen, davon 4 mit hoher Relevanz für Betreiber in DACH.

- SonicWall SMA1000: SSRF-Lücke höchster Schwere im Remote-Access-Gateway (CVE-2026-102255, 07.10.)
- Update: Hitachi Energy RTU500
- lwIP-SMTP-Client: kritischer Buffer Overflow (CVE-2026-15340, CVSS 9,8, ICSA-26-279-02, 06.10.)
- Hitachi Energy Asset Suite: Servlets ohne Anmeldung erreichbar, noch kein Patch (ICSA-26-279-03, 06.10.)

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	SonicWall SMA1000: SSRF-Lücke höchster Schwere im Remote-Access-Gateway (CVE-2026-102255, 07.10.)	HOCH
L-02	Atlassian Data Center: Angriffsversuche zwei Stunden nach PoC (CVE-2026-21589, 07.10.)	MITTEL
L-03	Schweiz und Österreich: tausende Windows-Fernzugänge offen im Internet (Analyse vom 05.10.)	MITTEL
L-04	Qilin-Ransomware: Japan liefert mutmaßlichen Täter an Deutschland aus	MITTEL
L-05	Update: Hitachi Energy RTU500	HOCH
L-06	lwIP-SMTP-Client: kritischer Buffer Overflow (CVE-2026-15340, CVSS 9,8, ICSA-26-279-02, 06.10.)	HOCH
L-07	Hitachi Energy Asset Suite: Servlets ohne Anmeldung erreichbar, noch kein Patch (ICSA-26-279-03, 06.10.)	HOCH
L-08	Hitachi Energy SOI: Remote Code Execution über die eingebaute ActiveMQ-Komponente (CVE-2026-34197, CVSS 8,8, ICSA-26-279-04, 06.10.)	MITTEL
L-09	Johnson Controls EasyIO FG: fest eingebaute Zugangsdaten, kein Patch (ICSA-26-279-01, 06.10.)	MITTEL
L-10	Hitachi Energy REB500: Denial of Service im Sammelschienenschutz über libexpat (ICSA-26-279-05, 06.10.)	MITTEL
L-11	WaterISAC baut den Austausch von Threat Intelligence für Wasserversorger aus (Bericht vom 06.10.)	MITTEL

Meldungen im Detail

L-01 SonicWall SMA1000: SSRF-Lücke höchster Schwere im Remote-Access-Gateway (CVE-2026-102255, 07.10.)

Relevanz: **HOCH**

Ohne Anmeldung können Angreifer die Appliances SMA1000 6210, 7210 und 8200v dazu bringen, Anfragen in ihrem Auftrag zu stellen und interne Funktionen zu erreichen. Nicht betroffen sind die SMA-100-Serie und SSL-VPN auf SonicWall-Firewalls. Hotfixes gibt es seit 07.10.; eine Ausnutzung ist laut Bericht noch nicht bekannt. Shadowserver zählt über 400 aus dem Internet erreichbare SMA1000-Appliances, und Ransomware-Gruppen haben im Juli 2026 bereits zwei Zero-Days in SMA1000 ausgenutzt. Relevant für Stadtwerke, Wasserversorger und Industrie, wenn Dienstleister ihre Fernwartung über SMA1000 abwickeln: Hotfix sofort einspielen, Zugriffe prüfen, Fernwartung nur über Jump Host mit MFA (CC4 Secure Remote Access).

Quelle: <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-max-severity-ssrf-flaw-in-sma1000-gateways/>

L-02 Atlassian Data Center: Angriffsversuche zwei Stunden nach PoC (CVE-2026-21589, 07.10.)

Relevanz: **MITTEL**

Ohne Anmeldung lassen sich bestimmte Dateien im Web-Root abrufen, wenn der genaue Pfad bekannt ist. Betroffen sind die selbst betriebenen Data-Center-Versionen von Jira Software, Jira Service Management, Confluence, Bitbucket, Bamboo und Crowd sowie Crucible und Fisheye. Bei Crowd-Anbindung können Angreifer Zugangsdaten im Klartext auslesen und Admin-Konten anlegen. Zwei Stunden nach dem öffentlichen PoC registrierte ein Honeypot die ersten Angriffsversuche. Versorger und Maschinenbauer legen in Confluence und Jira oft Netzpläne und Anlagendokumentation ab: gefixte Versionen laut Atlassian-Bulletin einspielen oder die Instanz vom Internet trennen (CC5).

Quelle: <https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-atlassian-flaw-after-public-poc-release/>

L-03 Schweiz und Österreich: tausende Windows-Fernzugänge offen im Internet (Analyse vom 05.10.)

Relevanz: **MITTEL**

Laut dem österreichischen Unternehmen Risikomonitor sind in der Schweiz 6.431 RDP-Zugänge offen erreichbar, 1.458 davon bauen eine Sitzung ohne vorherige Authentifizierung auf. Das sind 27,1 % der Schweizer Fernzugänge, in Österreich 20,5 %. Als Ursachen nennt die Analyse Standardeinstellungen der Internet-Anbieter und veraltete Systeme und empfiehlt VPN und Mehrfaktor-Authentifizierung. Energie und Wasser werden nicht einzeln ausgewiesen. Unsere Empfehlung: RDP nie direkt ins Internet, Fernzugänge von außen prüfen lassen (CC2, CC4).

Quelle: <https://persoenlich.com/digital/tausende-schweizer-rechner-sind-ungeschutzt>

L-04 Qilin-Ransomware: Japan liefert mutmaßlichen Täter an Deutschland aus

Relevanz: MITTEL

Ein 28-jähriger Russe soll laut heise ein wichtiger Teil der Gruppe Qilin sein, die Software programmiert und im September 2024 selbst die Systeme eines deutschen Logistikunternehmens manipuliert haben; das Unternehmen zahlte Lösegeld. Es gilt die Unschuldsvermutung. Solche Auslieferungen sind laut heise außergewöhnlich selten. Unsere Einschätzung: ein seltener Erfolg der Strafverfolgung, an der Bedrohungslage ändert er kurzfristig wenig – ein geübter Notfallplan bleibt Pflicht (CC1).

Quelle: <https://www.heise.de/news/Seltene-Sache-Japan-liefert-Ransomware-Verdaechtigen-an-Deutschland-aus-11478517.html>

L-05 Update: Hitachi Energy RTU500

Relevanz: HOCH

CISA veröffentlicht die Details zu den Lücken in alter CMU-Firmware (ICSA-26-279-06, 06.10.; Hersteller-Advisory vom 29.09.) – Betroffen ist die CMU-Firmware 11.x und älter, die End-of-Life ist. CISA listet sechs Schwachstellen: CVE-2026-8065 und CVE-2026-8066 (je CVSS 9,1), CVE-2010-2965 (CVSS 9,8), CVE-2014-9195 (8,1), CVE-2023-46143 (7,5) und CVE-2026-8067 (6,5). Möglich sind unter anderem Firmware-Uploads ohne Anmeldung, Firmware-Änderungen ohne Integritätsprüfung, das Überschreiben von Dateien und das Ausführen von Befehlen. Abhilfe ist nur das Upgrade auf 12.7.8, 13.9.1 oder neuer. Neu gegenüber unserer Wochenlage KW 40 sind die vollständige CVE-Liste und die Fix-Versionen. RTU500 steckt in vielen Umspannwerken und in der Fernwirktechnik von Stadtwerken – ein Abgleich der Firmware-Stände im Asset-Inventar lohnt sich.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-06>

L-06 lwIP-SMTP-Client: kritischer Buffer Overflow (CVE-2026-15340, CVSS 9,8, ICSA-26-279-02, 06.10.)

Relevanz: HOCH

Laut CISA kann der Fehler in lwIP 2.2.1 das Gerät abstürzen lassen, der Buffer Overflow könnte Remote Code Execution ermöglichen. CISA nennt die Sektoren Energie sowie Wasser/Abwasser. Der Fix liegt als Patch bzw. Git-Commit vor; Gerätehersteller müssen ihn erst in ihre Firmware übernehmen. Unsere Einschätzung: lwIP ist ein verbreiteter TCP/IP-Stack für Embedded-Geräte – Betreiber sollten ihre Lieferanten nach SBOM und Betroffenheit fragen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-02>

L-07 Hitachi Energy Asset Suite: Servlets ohne Anmeldung erreichbar, noch kein Patch (ICSA-26-279-03, 06.10.)

Relevanz: HOCH

In Version 9.9.0 und älter ist das HTTPPublishAdapterTestServlet ohne Anmeldung erreichbar, was Informationen preisgeben und die Integrität gefährden kann (CVE-2026-7395, CVSS 8,1). Über weitere ungeschützte Servlets ist ein Denial of Service möglich (CVE-2026-11796, CVSS 4,3). Version 9.9.1 kommt laut CISA erst „when available“; bis dahin sollen die betroffenen Servlets abgeschaltet werden. Asset Suite ist ein EAM-System, mit dem Energieversorger Instandhaltung und Anlagen verwalten.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-03>

L-08 Hitachi Energy SOI: Remote Code Execution über die eingebaute ActiveMQ-Komponente (CVE-2026-34197, CVSS 8,8, ICSA-26-279-04, 06.10.)

Relevanz: MITTEL

Ein angemeldeter Angreifer kann über eine Lücke in Apache ActiveMQ Code ausführen. Betroffen sind SOI 2.0.0 bis 2.2.0; der Patch SOI EP2 hebt ActiveMQ für den SOI Core auf 5.19.5. Nach Armatura One (OT-Lage 02.10.) ist das die zweite ActiveMQ-Lücke in OT-Produkten binnen einer Woche. Unsere Einschätzung: Drittkomponenten wie Message Broker gehören mit Version ins Asset-Inventar.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-04>

L-09 Johnson Controls EasyIO FG: fest eingebaute Zugangsdaten, kein Patch (ICSA-26-279-01, 06.10.)

Relevanz: MITTEL

Über CVE-2026-27872 und CVE-2026-27873 (je CVSS 7,7) ist ein vollständiger unberechtigter Zugriff auf den Controller möglich. Betroffen ist Firmware bis 2.0b52; die FG-Serie ist End-of-Life und End-of-Support, Patches gibt es nicht. Empfohlen sind die Migration auf neuere Produkte und bis dahin Segmentierung und Zugriffsbeschränkung. Nicht zu verwechseln mit EasyIO Neo aus der OT-Lage vom 02.10. Relevant für Gebäudeleittechnik in Wasserwerken, Bädern und kommunalen Liegenschaften.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-01>

L-10 Hitachi Energy REB500: Denial of Service im Sammelschienenschutz über libexpat (ICSA-26-279-05, 06.10.)

Relevanz: MITTEL

Zwei Lücken (CVE-2024-8176, CVE-2025-59375, je CVSS 6,5) können zu Denial of Service führen, CVE-2024-8176 je nach Umgebung auch zu Speicherkorruption. Betroffen ist Version 8.3.3.1 und älter, behoben in 8.3.4.0. Ausnutzbar nur mit Anmeldung, betroffen sind aber Schutzgeräte in Umspannwerken – das Update gehört in den nächsten Wartungsplan.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-05>

L-11 WaterISAC baut den Austausch von Threat Intelligence für Wasserversorger aus (Bericht vom 06.10.)

Relevanz: MITTEL

WaterISAC arbeitet dafür mit Cyware zusammen. WaterISAC verweist ausdrücklich auf den Konflikt mit Iran; Warnungen sollen Versorger in Stunden statt Wochen erreichen. Unsere Einschätzung: Für kleine Versorger in DACH gibt es ein vergleichbares Angebot bisher kaum.

Quelle: <https://route-fifty.com/cybersecurity/2026/10/new-partnership-formed-share-cyber-threat-intel-water-utilities/416438>

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