OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 13.11.2026, 16:35 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	13.11.2026
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 2 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• **Citrix NetScaler ADC und Gateway: Security Bulletin mit 28 Lücken (CTX697305)**: Die Cloud Software Group hat ein Sammel-Bulletin für NetScaler ADC und NetScaler Gateway veröffentlicht

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**Citrix NetScaler ADC und Gateway: Security Bulletin mit 28 Lücken (CTX697305)**: Die Cloud Software Group hat ein Sammel-Bulletin für NetScaler ADC und NetScaler Gateway veröffentlicht	HOCH
L-02	**CISA „Installed Base Program“: US-Behörde arbeitet mit OT-Herstellern an verwundbaren Geräten im Netz**: Die US-Behörde arbeitet mit OT-Herstellern (OEMs) zusammen, die Hersteller beteiligen sich freiwillig	MITTEL

Meldungen im Detail

L-01 **Citrix NetScaler ADC und Gateway: Security Bulletin mit 28 Lücken (CTX697305)**: Die Cloud Software Group hat ein Sammel-Bulletin für NetScaler ADC und NetScaler Gateway veröffentlicht

Relevanz: HOCH

Es listet 28 CVEs, die meisten mit CVSS 4.0 von 8,7 oder 9,3, die höchste mit 9,5. Laut Bulletin betroffen sind die Versionen 14.1 vor 14.1-73.57 und 13.1 vor 13.1-64.39 sowie die FIPS- und NDcPP-Builds. Behoben ist das ab 14.1-73.57, 13.1-64.39, 14.1-73.58 FIPS und 13.1-37.293 FIPS/NDcPP. Die Lücken liegen unter anderem in der Gateway-Authentisierung (SAML, LDAP, E-Mail-OTP), in Endpoint Analysis und im ICA-Proxy. Eine Ausnutzung erwähnt das Bulletin nicht. Das Bulletin rät dringend, so schnell wie möglich zu aktualisieren. Unsere Einschätzung: Wo NetScaler-Gateways bei Stadtwerken und Versorgern als Remote-Access-Zugang für Dienstleister dienen, können sie je nach Segmentierung ein Weg in die Leittechnik sein. Wir empfehlen, diese Geräte mit Vorrang zu patchen (CC4 Secure Remote Access der SANS Five ICS Critical Controls).

Quelle: https://support.citrix.com/external/article/CTX697305

L-02 **CISA „Installed Base Program“: US-Behörde arbeitet mit OT-Herstellern an verwundbaren Geräten im Netz**: Die US-Behörde arbeitet mit OT-Herstellern (OEMs) zusammen, die Hersteller beteiligen sich freiwillig

Relevanz: MITTEL

Ziel ist es, verwundbare OT-Geräte zu finden, die aus dem Internet erreichbar sind, und ihre Betreiber zu warnen, bevor die Lücken ausgenutzt werden. Als Beispiele nennt CISA Energie und Wasser. Einen Starttermin oder Partnerfirmen haben wir auf der CISA-Seite nicht gefunden. Das Programm richtet sich an US-Betreiber kritischer Infrastruktur. Unsere Einschätzung: Es zeigt, wohin es geht. Hersteller helfen beim Asset-Inventar für Geräte, die ihre Kunden ins Netz gestellt haben.

Quelle: https://www.cisa.gov/resources-tools/programs/installed-base-program

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