

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 23.10.2026, 16:17 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	23.10.2026
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 12 Meldungen, davon 5 mit hoher Relevanz für Betreiber in DACH.

- **Fortinet:** außerplanmäßige Updates für FortiOS, FortiManager, FortiAnalyzer, FortiMail und FortiAuthenticator (21./22.10.) Laut Fortinet sollen seit 21.10. (FortiMail, FortiAuthenticator) bzw. 22.10. (übrige Produkte) Updates bereitstehen, die kritische und hoch eingestufte Lücken schließen sollen. Aufgefallen sind sie bei KI-gestützten Sicherheitstests. Die Fixversionen sind FortiOS 8.0.2, 7.6.8, 7.4.13 und 7.2.14, FortiManager und FortiAnalyzer 8.0.2, 7.6.8, 7.4.12 und 7.2.13, FortiMail 8.0.2, 7.6.7 und 7.4.9 (wer 7.2 nutzt, soll auf 7.4 wechseln) sowie FortiAuthenticator 8.0.4 und 6.6.11. Sicherheitsmitteilungen mit Details will Fortinet erst am Patchday am 10.11.2026 veröffentlichen. Zu einer Ausnutzung äußert sich Fortinet nicht, warnt aber, dass Angreifer über Patch-Diffing schnell Exploits bauen können. Fortinet rät, zuerst die aus dem Internet erreichbaren Geräte zu aktualisieren und den Admin-Zugriff per HTTPS und SSH auf vertrauenswürdige IP-Adressen zu beschränken oder auf externen Interfaces abzuschalten. Unsere Einschätzung: FortiGate ist häufig auch bei Stadtwerken und Versorgern im Einsatz, dort sollte das Update jetzt eingeplant werden (CC5 Risk-Based Vulnerability Management). Quelle: <https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products> · <https://www.heise.de/news/Ausserplanmaessige-Fortinet-Updates-Details-Fehlanzeige-aber-dringend-11497171.html>
- **Forescout:** weltweit tausende Kühlsteuerungen offen im Internet (22./23.10.) Vedere Labs von Forescout zählt 12.976 aus dem Internet erreichbare Dienste von Kühlsteuerungen auf 6.017 IP-Adressen in 99 Ländern und Territorien. Die meisten entfallen auf Copeland/Dixell XWEB (7.075) und Danfoss StoreView (4.697). 3.762 StoreView-Dienste, also rund 80 %, laufen mit Firmware älter als 4.3.1 und sind damit potenziell von CVE-2025-41451 und CVE-2025-41452 betroffen. Seit Januar 2026 hat Forescout über 20 Angriffe auf Kühlanlagen gezählt, zu denen sich Hacktivist*innen bekannt haben, die Ziele lagen unter anderem in Spanien und Italien. Besonders aktiv waren die prorussischen Gruppen Z-Pentest Alliance und NoName057(16). Hintergrund sind Angriffe in Frankreich, bei denen laut Industrial Cyber in über 700 Supermärkten Kühlsteuerungen manipuliert worden sein sollen. Die Forscher warnen, dass neben Supermärkten auch Lebensmittelverarbeitung, Landwirtschaft und Krankenhäuser betroffen sein können. Unsere Einschätzung: Auch in DACH setzen Lebensmittelbetriebe und Krankenhäuser solche Steuerungen ein, Zahlen für DACH nennen die Berichte nicht. Forescout empfiehlt, die Management-Oberflächen nicht direkt aus dem Internet erreichbar zu machen, sichere Remote-Access-Gateways zu nutzen, die Anmeldung externer Dienstleister zu härten und Änderungen an Temperaturen, Abtauzeiten und Alarmen zu überwachen (CC4 Secure Remote Access). Die Zahlen stammen aus den übereinstimmenden Berichten von Industrial Cyber und IT Security Guru, den Forescout-Bericht selbst haben wir nicht eingesehen. Quelle: <https://industrialcyber.co/industrial-cyber-attacks/forescout-warns-internet-exposed-refrigeration-controls-could-enable-attacks-on-food-supply-chains-and-hospitals/> · <https://www.itsecurityguru.org/2026/10/22/exposed-refrigeration-systems-forescout-research/>
- ****Arista VeloCloud Orchestrator:** Zero-Day wird aktiv ausgenutzt (CVE-2026-114625, 22.10.)**
- ****Siemens SIMATIC S7-1500 und ET 200SP:** acht Lücken im Webserver (ICSA-26-295-14, 22.10.)**
- ****Siemens SIMATIC WinCC:** Rechteauserweiterung bis zur Befehlsausführung auf dem Host, für V7.5 kein Fix (CVE-2026-59241, CVSS 8,8, ICSA-26-295-13)**

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	<p>Fortinet: außerplanmäßige Updates für FortiOS, FortiManager, FortiAnalyzer, FortiMail und FortiAuthenticator (21./22.10.) Laut Fortinet sollen seit 21.10. (FortiMail, FortiAuthenticator) bzw. 22.10. (übrige Produkte) Updates bereitstehen, die kritische und hoch eingestufte Lücken schließen sollen. Aufgefallen sind sie bei KI-gestützten Sicherheitstests. Die Fixversionen sind FortiOS 8.0.2, 7.6.8, 7.4.13 und 7.2.14, FortiManager und FortiAnalyzer 8.0.2, 7.6.8, 7.4.12 und 7.2.13, FortiMail 8.0.2, 7.6.7 und 7.4.9 (wer 7.2 nutzt, soll auf 7.4 wechseln) sowie FortiAuthenticator 8.0.4 und 6.6.11. Sicherheitsmitteilungen mit Details will Fortinet erst am Patchday am 10.11.2026 veröffentlichen. Zu einer Ausnutzung äußert sich Fortinet nicht, warnt aber, dass Angreifer über Patch-Diffing schnell Exploits bauen können. Fortinet rät, zuerst die aus dem Internet erreichbaren Geräte zu aktualisieren und den Admin-Zugriff per HTTPS und SSH auf vertrauenswürdige IP-Adressen zu beschränken oder auf externen Interfaces abzuschalten. Unsere Einschätzung: FortiGate ist häufig auch bei Stadtwerken und Versorgern im Einsatz, dort sollte das Update jetzt eingeplant werden (CC5 Risk-Based Vulnerability Management). Quelle: https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products · https://www.heise.de/news/Ausserplanmaessige-Fortinet-Updates-Details-Fehlanzeige-aber-dringend-11497171.html</p>	HOCH
L-02	<p>Forescout: weltweit tausende Kühlsteuerungen offen im Internet (22./23.10.) Vedere Labs von Forescout zählt 12.976 aus dem Internet erreichbare Dienste von Kühlsteuerungen auf 6.017 IP-Adressen in 99 Ländern und Territorien. Die meisten entfallen auf Copeland/Dixell XWEB (7.075) und Danfoss StoreView (4.697). 3.762 StoreView-Dienste, also rund 80 %, laufen mit Firmware älter als 4.3.1 und sind damit potenziell von CVE-2025-41451 und CVE-2025-41452 betroffen. Seit Januar 2026 hat Forescout über 20 Angriffe auf Kühlanlagen gezählt, zu denen sich Hacktivist*innen bekannt haben, die Ziele lagen unter anderem in Spanien und Italien. Besonders aktiv waren die prorussischen Gruppen Z-Pentest Alliance und NoName057(16). Hintergrund sind Angriffe in Frankreich, bei denen laut Industrial Cyber in über 700 Supermärkten Kühlsteuerungen manipuliert worden sein sollen. Die Forscher warnen, dass neben Supermärkten auch Lebensmittelverarbeitung, Landwirtschaft und Krankenhäuser betroffen sein können. Unsere Einschätzung: Auch in DACH setzen Lebensmittelbetriebe und Krankenhäuser solche Steuerungen ein, Zahlen für DACH nennen die Berichte nicht. Forescout empfiehlt, die Management-Oberflächen nicht direkt aus dem Internet erreichbar zu machen, sichere Remote-Access-Gateways zu nutzen, die Anmeldung externer Dienstleister zu härten und Änderungen an Temperaturen, Abtauzeiten und Alarmen zu überwachen (CC4 Secure Remote Access). Die Zahlen stammen aus den übereinstimmenden Berichten von Industrial Cyber und IT Security Guru, den Forescout-Bericht selbst haben wir nicht eingesehen. Quelle: https://industrialcyber.co/industrial-cyber-attacks/forescout-warns-internet-exposed-refrigeration-controls-could-enable-attacks-on-food-supply-chains-and-hospitals/ · https://www.itsecurityguru.org/2026/10/22/exposed-refrigeration-systems-forescout-research/</p>	HOCH

ID	Meldung	Relevanz
L-03	HPE Aruba AOS-8 und AOS-10: acht Lücken mit höchstem Schweregrad (Bericht vom 23.10.) Laut BleepingComputer hat HPE 72 Lücken in ArubaOS geschlossen, darunter acht mit höchstem Schweregrad (CVE-2026-79844 bis CVE-2026-79851). Es geht um mehrere Authentication Bypasses (u. a. im PAPI-Protokoll) sowie um Command Injection, SQL-Injection und Buffer Overflows ohne Anmeldung, die meist zur Codeausführung führen. ArubaOS läuft auf Mobility Conductors, Controllern, Access Points und Gateways. Laut HPE gibt es bisher keinen öffentlichen Exploit-Code und keine bekannte Ausnutzung. HPE rät, CLI und Web-Management auf ein eigenes Layer-2-Segment bzw. VLAN zu beschränken oder per Firewall-Regeln abzusichern. Unsere Einschätzung: Aruba-WLAN steht oft auch in Betriebsnetzen von Versorgern und in der Produktion, dort gehört das Update auf die Liste (CC5 Risk-Based Vulnerability Management). Quelle: https://www.bleepingcomputer.com/news/security/hpe-patches-eight-max-severity-rce-and-auth-bypass-aos-flaws/	MITTEL
L-04	Columbia (South Carolina): Cyber-Vorfall legt städtische Online-Dienste lahm (Bericht vom 22.10.) Laut The Record sind das Bürgerportal MyColaSC (dort zahlen Bürger unter anderem Versorgerrechnungen), das GIS und Systeme des Tierschutzdiensts ausgefallen. Die Ermittlungen führt die Landespolizei SLED. Nach Angaben der Stadt laufen Polizei, Feuerwehr, Notruf 911, die Systeme von Columbia Water und das Zahlungszentrum weiter. Ob es Ransomware war, hat die Stadt nicht beantwortet, bekannt hatte sich bis Mittwoch niemand. Unsere Einschätzung: Für Stadtwerke zeigt der Fall, wie wichtig die Trennung zwischen der IT der Stadtverwaltung und den Systemen des Versorgers ist (CC2 Defensible Architecture). Quelle: https://therecord.media/south-carolina-officials-offer-assistance-cyber-incident	MITTEL
L-05	Unbestätigt, nur eine Quelle: Ransomware-Gruppe N0n beansprucht Angriff auf ein Schweizer Solarenergie-Unternehmen (20.10.) Laut DeXpose hat die Gruppe N0n einen Angriff auf ein Solarenergie-Unternehmen in der Schweiz behauptet und droht mit der Veröffentlichung von Daten. Einen Namen nennt DeXpose nicht, nur „Company #95“. Eine Bestätigung des Unternehmens oder weitere Quellen liegen uns nicht vor. Quelle: https://www.dexpose.io/n0n-ransomware-group-targets-swiss-solar-energy-firm/	NIEDRIG
L-06	**Arista VeloCloud Orchestrator: Zero-Day wird aktiv ausgenutzt (CVE-2026-114625, 22.10.)**	HOCH
L-07	**Siemens SIMATIC S7-1500 und ET 200SP: acht Lücken im Webserver (ICSA-26-295-14, 22.10.)**	HOCH
L-08	**Siemens SIMATIC WinCC: Rechteauserweiterung bis zur Befehlsausführung auf dem Host, für V7.5 kein Fix (CVE-2026-59241, CVSS 8,8, ICSA-26-295-13)**	HOCH
L-09	**Siemens APOGEE, TALON und Desigo PXC/PXM: DoS ohne Anmeldung, für einen Teil der Geräte ist kein Fix geplant (ICSA-26-295-08)**	MITTEL
L-10	**Siemens RUGGEDCOM CROSSBOW: elf Lücken, u. a. SQL-Injection (ICSA-26-295-12)**	MITTEL
L-11	**Siemens S7-1500 CPU 1518(F)-4 PN/DP MFP: 428 Lücken im Linux-Subsystem, CVSS 10, noch kein Fix (ICSA-26-295-11)**	MITTEL
L-12	**Weitere Siemens-Advisories vom 22.10.**	MITTEL

Meldungen im Detail

L-01 Fortinet: außerplanmäßige Updates für FortiOS, FortiManager, FortiAnalyzer, FortiMail und FortiAuthenticator (21./22.10.) Laut Fortinet sollen seit 21.10. (FortiMail, FortiAuthenticator) bzw. 22.10. (übrige Produkte) Updates bereitstehen, die kritische und hoch eingestufte Lücken schließen sollen. Aufgefallen sind sie bei KI-gestützten Sicherheitstests. Die Fixversionen sind FortiOS 8.0.2, 7.6.8, 7.4.13 und 7.2.14, FortiManager und FortiAnalyzer 8.0.2, 7.6.8, 7.4.12 und 7.2.13, FortiMail 8.0.2, 7.6.7 und 7.4.9 (wer 7.2 nutzt, soll auf 7.4 wechseln) sowie FortiAuthenticator 8.0.4 und 6.6.11. Sicherheitsmitteilungen mit Details will Fortinet erst am Patchday am 10.11.2026 veröffentlichen. Zu einer Ausnutzung äußert sich Fortinet nicht, warnt aber, dass Angreifer über Patch-Diffing schnell Exploits bauen können. Fortinet rät, zuerst die aus dem Internet erreichbaren Geräte zu aktualisieren und den Admin-Zugriff per HTTPS und SSH auf vertrauenswürdige IP-Adressen zu beschränken oder auf externen Interfaces abzuschalten. Unsere Einschätzung: FortiGate ist häufig auch bei Stadtwerken und Versorgern im Einsatz, dort sollte das Update jetzt eingeplant werden (CC5 Risk-Based Vulnerability Management). Quelle: <https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products> · <https://www.heise.de/news/Ausserplanmaessige-Fortinet-Updates-Details-Fehlannonce-aber-dringen-d-11497171.html>

Relevanz: **HOCH**

L-02 Forescout: weltweit tausende Kühlsteuerungen offen im Internet (22./23.10.) Vedere Labs von Forescout zählt 12.976 aus dem Internet erreichbare Dienste von Kühlsteuerungen auf 6.017 IP-Adressen in 99 Ländern und Territorien. Die meisten entfallen auf Copeland/Dixell XWEB (7.075) und Danfoss StoreView (4.697). 3.762 StoreView-Dienste, also rund 80 %, laufen mit Firmware älter als 4.3.1 und sind damit potenziell von CVE-2025-41451 und CVE-2025-41452 betroffen. Seit Januar 2026 hat Forescout über 20 Angriffe auf Kühlanlagen gezählt, zu denen sich Hacktivist*innen bekannt haben, die Ziele lagen unter anderem in Spanien und Italien. Besonders aktiv waren die prorussischen Gruppen Z-Pentest Alliance und NoName057(16). Hintergrund sind Angriffe in Frankreich, bei denen laut Industrial Cyber in über 700 Supermärkten Kühlsteuerungen manipuliert worden sein sollen. Die Forscher warnen, dass neben Supermärkten auch Lebensmittelverarbeitung, Landwirtschaft und Krankenhäuser betroffen sein können. Unsere Einschätzung: Auch in DACH setzen Lebensmittelbetriebe und Krankenhäuser solche Steuerungen ein, Zahlen für DACH nennen die Berichte nicht. Forescout empfiehlt, die Management-Oberflächen nicht direkt aus dem Internet erreichbar zu machen, sichere Remote-Access-Gateways zu nutzen, die Anmeldung externer Dienstleister zu härten und Änderungen an Temperaturen, Abtauzeiten und Alarmen zu überwachen (CC4 Secure Remote Access). Die Zahlen stammen aus den übereinstimmenden Berichten von Industrial Cyber und IT Security Guru, den Forescout-Bericht selbst haben wir nicht eingesehen. Quelle: <https://industrialcyber.co/industrial-cyber-attacks/forescout-warns-internet-exposed-refrigeration-controls-could-enable-attacks-on-food-supply-chains-and-hospitals/> · <https://www.itsecurityguru.org/2026/10/22/exposed-refrigeration-systems-forescout-research/>

Relevanz: **HOCH**

L-03 HPE Aruba AOS-8 und AOS-10: acht Lücken mit höchstem Schweregrad (Bericht vom 23.10.) Laut BleepingComputer hat HPE 72 Lücken in ArubaOS geschlossen, darunter acht mit höchstem Schweregrad (CVE-2026-79844 bis CVE-2026-79851). Es geht um mehrere Authentication Bypasses (u. a. im PAPI-Protokoll) sowie um Command Injection, SQL-Injection und Buffer Overflows ohne Anmeldung, die meist zur Codeausführung führen. ArubaOS läuft auf Mobility Conductors, Controllern, Access Points und Gateways. Laut HPE gibt es bisher keinen öffentlichen Exploit-Code und keine bekannte Ausnutzung. HPE rät, CLI und Web-Management auf ein eigenes Layer-2-Segment bzw. VLAN zu beschränken oder per Firewall-Regeln abzusichern. Unsere Einschätzung: Aruba-WLAN steht oft auch in Betriebsnetzen von Versorgern und in der Produktion, dort gehört das Update auf die Liste (CC5 Risk-Based Vulnerability Management). Quelle: <https://www.bleepingcomputer.com/news/security/hpe-patches-eight-max-severity-rce-and-auth-bypass-aos-flaws/>

Relevanz: **MITTEL**

L-04 Columbia (South Carolina): Cyber-Vorfall legt städtische Online-Dienste lahm (Bericht vom 22.10.) Laut The Record sind das Bürgerportal MyColaSC (dort zahlen Bürger unter anderem Versorgerrechnungen), das GIS und Systeme des Tierschutzdiensts ausgefallen. Die Ermittlungen führt die Landespolizei SLED. Nach Angaben der Stadt laufen Polizei, Feuerwehr, Notruf 911, die Systeme von Columbia Water und das Zahlungszentrum weiter. Ob es Ransomware war, hat die Stadt nicht beantwortet, bekannt hatte sich bis Mittwoch niemand. Unsere Einschätzung: Für Stadtwerke zeigt der Fall, wie wichtig die Trennung zwischen der IT der Stadtverwaltung und den Systemen des Versorgers ist (CC2 Defensible Architecture). Quelle: <https://therecord.media/south-carolina-officials-offer-assistance-cyber-incident>

Relevanz: MITTEL

L-05 Unbestätigt, nur eine Quelle: Ransomware-Gruppe N0n beansprucht Angriff auf ein Schweizer Solarenergie-Unternehmen (20.10.) Laut DeXpose hat die Gruppe N0n einen Angriff auf ein Solarenergie-Unternehmen in der Schweiz behauptet und droht mit der Veröffentlichung von Daten. Einen Namen nennt DeXpose nicht, nur „Company #95“. Eine Bestätigung des Unternehmens oder weitere Quellen liegen uns nicht vor. Quelle: <https://www.dexpose.io/n0n-ransomware-group-targets-swiss-solar-energy-firm/>

Relevanz: NIEDRIG

L-06 **Arista VeloCloud Orchestrator: Zero-Day wird aktiv ausgenutzt (CVE-2026-114625, 22.10.)**

Relevanz: HOCH

Über eine SQL-Injection im On-Prem-Orchestrator (SD-WAN) kann laut Arista jedes angemeldete Konto Operator-Rechte erlangen. Gepatcht ist in 5.2.3.18, 6.1.3.10 und 6.4.2.12; gehostete Instanzen hat Arista selbst aktualisiert, On-Prem-Betreiber müssen selbst updaten. Zwei frühere VCO-Lücken (CVE-2026-16812 und CVE-2026-93952) hat CISA schon in den KEV-Katalog der aktiv ausgenutzten Lücken aufgenommen. Unsere Einschätzung: Wer Außenstellen, Pumpwerke oder Umspannwerke per VeloCloud-SD-WAN anbindet, sollte die Version jetzt prüfen. CVSS 9,9 laut securityonline, BleepingComputer stuft die Lücke als „critical“ ein.

Quelle: <https://www.bleepingcomputer.com/news/security/arista-patches-new-velocloud-orchestrator-zero-day-exploited-in-attacks/>

Quelle: <https://securityonline.info/velocloud-orchestrator-cve-2026-114625-exploited/>

L-07 **Siemens SIMATIC S7-1500 und ET 200SP: acht Lücken im Webserver (ICSA-26-295-14, 22.10.)**

Relevanz: **HOCH**

CVE-2026-63350 bis -63357 betreffen laut Advisory zahlreiche S7-1500- und ET-200SP-Produkte, CVSS bis 9,6. Für die aufgeführten Produkte nennt das Advisory derzeit keinen Fix und empfiehlt Mitigationen. Ein Angreifer bringt einen Nutzer mit dem Recht „Read diagnostics“ dazu, eine präparierte Trace-Datei zu importieren, und kann dann mit dessen Rechten Aktionen auf der SPS ausführen. Bis zum Fix empfiehlt Siemens unter anderem, den Webserver abzuschalten, wo er nicht gebraucht wird (Ports 80/tcp und 443/tcp).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-14>

L-08 **Siemens SIMATIC WinCC: Rechteausweitung bis zur Befehlsausführung auf dem Host, für V7.5 kein Fix (CVE-2026-59241, CVSS 8,8, ICSA-26-295-13)**

Relevanz: **HOCH**

Eine Datenbankrolle hat zu viele Rechte, dadurch kann ein angemeldeter Nutzer mit Datenbankzugriff Befehle auf dem System ausführen. Behoben ist es in V8.0 Update 11 und V8.1 Update 7. Für V7.5 gibt es derzeit keinen Fix, Siemens empfiehlt Mitigationen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-13>

L-09 **Siemens APOGEE, TALON und Desigo PXC/PXM: DoS ohne Anmeldung, für einen Teil der Geräte ist kein Fix geplant (ICSA-26-295-08)**

Relevanz: **MITTEL**

Es geht um fünf CVEs, u. a. in der Paketverarbeitung (CVE-2026-89208, -102073 bis -102076, CVSS bis 8,2). Für einen Teil der Geräte bietet Siemens Updates an (V3.5.7 bzw. V2.8.21). Unsere Einschätzung: Wer diese Controller in der Gebäudeautomation von Klärwerken, Wasserwerken oder Leitstellen einsetzt, sollte prüfen. Empfehlung laut Advisory: segmentieren, Controller hinter Firewalls, FTP/Web abgeschaltet lassen (Standard bei APOGEE, Desigo und TALON).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-08>

L-10 **Siemens RUGGEDCOM CROSSBOW: elf Lücken, u. a. SQL-Injection (ICSA-26-295-12)**

Relevanz: **MITTEL**

Mit CVE-2026-89196 bis -89206 (CVSS bis 8,8) können angemeldete Nutzer mit bestimmten, teils administrativen Rechten beliebige SQL-Befehle auf der Datenbank ausführen und sensible Verwaltungsdaten auslesen. Betroffen sind alle Versionen vor V6.0, der Fix ist V6.0. Unsere Einschätzung: Wer CROSSBOW für die Fernwartung im Umspannwerk nutzt, sollte V6.0 zügig einspielen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-12>

L-11 **Siemens S7-1500 CPU 1518(F)-4 PN/DP MFP: 428 Lücken im Linux-Subsystem, CVSS 10, noch kein Fix (ICSA-26-295-11)**

Relevanz: MITTEL

Betroffen ist Firmware ab V3.1.7. Siemens bereitet Fixes vor und empfiehlt bis dahin, den Zugang zur Shell des Linux-Subsystems auf vertrauenswürdigen Personal zu beschränken und nur Anwendungen aus vertrauenswürdigen Quellen zu bauen und auszuführen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-11>

L-12 **Weitere Siemens-Advisories vom 22.10.**

Relevanz: MITTEL

Für Netzplanung und Energie ist PSS SINCAL wichtig: Absturz über die WibuKey-Komponente, nur mit Legacy-Dongle-Lizenz (CVE-2026-84854, CVSS 7, Fix V22.5 Update 5; für V21.5 und V22.0 gibt es noch keinen Fix, Siemens nennt als Mitigation die WibuKey Runtime for Windows 6.72, <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-06>). Beim Industrial Edge App Publisher kann ein Angreifer im Netz den Management-Server vortäuschen und Code auf dem Rechner ausführen (CVE-2026-78556 und -78557, Fix V1.27.9, <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-02>). Bei SIMATIC IPCs lässt sich Secure Boot über einen Testschlüssel umgehen (CVE-2026-72895, Fix: Updates auf neue Versionen, <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-07>). Dazu kommt SENTRON 3NA COM (<https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-05>).

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