OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 05.11.2026, 16:04 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	05.11.2026
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 5 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

• Zyxel GS1900: Zero-Day in Switches ausgenutzt, fast 1.000 Geräte kompromittiert, Zyxel hat eine Lücke im Web-Management der Switch-Serie GS1900 geschlossen (laut BleepingComputer CVE-2026-107441, Out-of-bounds Write). Angreifer konnten damit ohne Anmeldung per präparierter HTTP-Anfrage Befehle ausführen und haben Konfigurationsdateien, gehashte Root-Zugangsdaten und Netzinformationen abgegriffen. Laut GreyNoise sind 996 Geräte in 48 Ländern betroffen, ausgenutzt seit etwa 17. August. Zyxel führt die Lücke als eigene Schwachstelle, weil der Exploit zusätzlich fehlende Längenprüfungen der HTTP-Parameter ausnutzt. Ob der Exploit gezielt gebaut wurde, um die Juni-Updates für CVE-2026-7273 zu umgehen, ist unklar. Betroffen sind zehn GS1900-Modelle; die Updates kamen am 22.10., das Advisory am 03.11. Wer GS1900 im eigenen Netz hat, auch in Anlagen- oder Stationsnetzen, sollte die Firmware vom 22.10. einspielen, die Management-Oberfläche nur aus einem Verwaltungsnetz erreichbar machen und die Zugangsdaten der Switches ändern (CC2 Defensible Architecture). Quelle: https://www.bleepingcomputer.com/news/security/zyxel-fixes-zero-day-exploited-to-hack-nearly-1-000-network-switches/

• Nach den Supermarkt-Angriffen: Kühllager des Blutspendedienstes EFS betroffen (02.11.), Betroffen sind Kühllager des staatlichen Blutspendeinstituts EFS; laut BleepingComputer war nicht EFS selbst das Ziel, sondern ein Kühl-Dienstleister. Unabhängig davon bestätigte Coolworld Rentals einen Vorfall mit seiner Fernüberwachungs-Software (laut Coolworld über eine Lücke in der Komponente eines Drittanbieters); ob Coolworld der Dienstleister der EFS ist, ist nicht bestätigt, EFS nennt ihn nicht. In drei Einrichtungen wurden Temperatur- und Abtau-Grenzwerte auf extrem hohe Werte gestellt. Laut EFS gingen keine Blutprodukte verloren, EFS arbeitet mit der ANSSI und dem Gesundheitsministerium zusammen. Ob die Täter dieselbe Methode wie bei den Supermarkt-Angriffen genutzt haben, ist nicht bestätigt. Für DACH zeigt der Fall, dass Fernüberwachung und Fernzugriff von Dienstleistern auch Kühlketten in Kliniken, Pharma und Lebensmitteln treffen können (CC4 Secure Remote Access). Quelle: https://www.bleepingcomputer.com/news/security/cyberattack-disrupts-blood-storage-refrigeration-systems-in-france/

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	Phoenix Contact PLCnext Engineer: drei Lücken in der Engineering-Software (CERT@VDE VDE-2026-121, 04.11.2026). Betroffen sind alle Versionen vor 2026.6. Über manipulierte Plug-in-Pakete ist Codeausführung im Kontext des Nutzers möglich, gefälschte PROFINET-Gerätebeschreibungen (GSDML) werden als gültig signiert angezeigt, und es gibt eine Path-Traversal-Lücke. Betroffen sind CVE-2026-110935 und CVE-2026-110022 (CVSS 8,4) sowie CVE-2026-110021 (CVSS 6,2). Für CVE-2026-110935 und CVE-2026-110022 nennt das Advisory einen lokalen Angriffsvektor (AV:L). Meine Empfehlung (nicht aus der Quelle): Bis zum Update Plug-ins nur aus vertrauenswürdigen Quellen installieren und GSDML-Dateien nur aus Herstellerquellen importieren. Meine Einschätzung (nicht aus der Quelle): Das trifft die Engineering-Rechner von Integratoren und Betreibern mit PLCnext-Steuerungen, also auch in der Wasserwirtschaft. Quelle: https://certvde.com/en/advisories/VDE-2026-121/	MITTEL
L-02	Zyxel GS1900: Zero-Day in Switches ausgenutzt, fast 1.000 Geräte kompromittiert, Zyxel hat eine Lücke im Web-Management der Switch-Serie GS1900 geschlossen (laut BleepingComputer CVE-2026-107441, Out-of-bounds Write). Angreifer konnten damit ohne Anmeldung per präparierter HTTP-Anfrage Befehle ausführen und haben Konfigurationsdateien, gehashte Root-Zugangsdaten und Netzinformationen abgegriffen. Laut GreyNoise sind 996 Geräte in 48 Ländern betroffen, ausgenutzt seit etwa 17. August. Zyxel führt die Lücke als eigene Schwachstelle, weil der Exploit zusätzlich fehlende Längenprüfungen der HTTP-Parameter ausnutzt. Ob der Exploit gezielt gebaut wurde, um die Juni-Updates für CVE-2026-7273 zu umgehen, ist unklar. Betroffen sind zehn GS1900-Modelle; die Updates kamen am 22.10., das Advisory am 03.11. Wer GS1900 im eigenen Netz hat, auch in Anlagen- oder Stationsnetzen, sollte die Firmware vom 22.10. einspielen, die Management-Oberfläche nur aus einem Verwaltungsnetz erreichbar machen und die Zugangsdaten der Switches ändern (CC2 Defensible Architecture). Quelle: https://www.bleepingcomputer.com/news/security/zyxel-fixes-zero-day-exploited-to-hack-nearly-1-000-network-switches/	HOCH
L-03	Nach den Supermarkt-Angriffen: Kühllager des Blutspendedienstes EFS betroffen (02.11.), Betroffen sind Kühllager des staatlichen Blutspendeinstituts EFS; laut BleepingComputer war nicht EFS selbst das Ziel, sondern ein Kühl-Dienstleister. Unabhängig davon bestätigte Coolworld Rentals einen Vorfall mit seiner Fernüberwachungs-Software (laut Coolworld über eine Lücke in der Komponente eines Drittanbieters); ob Coolworld der Dienstleister der EFS ist, ist nicht bestätigt, EFS nennt ihn nicht. In drei Einrichtungen wurden Temperatur- und Abtau-Grenzwerte auf extrem hohe Werte gestellt. Laut EFS gingen keine Blutprodukte verloren, EFS arbeitet mit der ANSSI und dem Gesundheitsministerium zusammen. Ob die Täter dieselbe Methode wie bei den Supermarkt-Angriffen genutzt haben, ist nicht bestätigt. Für DACH zeigt der Fall, dass Fernüberwachung und Fernzugriff von Dienstleistern auch Kühlketten in Kliniken, Pharma und Lebensmitteln treffen können (CC4 Secure Remote Access). Quelle: https://www.bleepingcomputer.com/news/security/cyberattack-disrupts-blood-storage-refrigeration-systems-in-france/	HOCH

ID	Meldung	Relevanz
L-04	Barracuda Email Security Gateway & Co.: Lückenkette führt zu Root-Rechten, Zwei Lücken: CVE-2026-116606 (CVSS 9,3, Authentication Bypass, nur ESG) und CVE-2026-111560 (CVSS 8,6, Command Injection in der Zeitzonen-Einstellung). Die zweite trifft auch Load Balancer ADC, Message Archiver, WAF, WAF Control Center und Web Security Gateway. Patches gibt es; zu einer Ausnutzung machen weder Barracuda noch Mandiant eine Angabe. Unklar ist, ob die ESG-Lücke eine Anmeldung voraussetzt: Mandiant sagt, sie geht ohne Anmeldung. Barracuda verlangt im Advisory für beide Lücken Admin-Zugang, nennt CVE-2026-116606 aber zugleich „pre-authentication“. Quelle: https://www.securityweek.com/barracuda-email-security-gateway-authentication-bypass-opens-path-to-root/	MITTEL
L-05	SonicWall GMS: Zwei Lücken, es kommt kein Patch mehr (End of Life), CVE-2026-109593 (Dateien auslesen ohne Anmeldung) und CVE-2026-109594 (SQL Injection) betreffen GMS 9.5.2 und älter. GMS wird nicht mehr gepflegt, SonicWall rät zum Umstieg auf NSM. Zu einer Ausnutzung macht die Quelle keine Angabe. Wer seine SonicWall-Firewalls zentral über GMS verwaltet, sollte die Konsole abschotten und den Umzug planen. Quelle: https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-unpatched-flaws-in-end-of-life-gms-software/	MITTEL

Meldungen im Detail

L-01 Phoenix Contact PLCnext Engineer: drei Lücken in der Engineering-Software (CERT@VDE VDE-2026-121, 04.11.2026). Betroffen sind alle Versionen vor 2026.6. Über manipulierte Plug-in-Pakete ist Codeausführung im Kontext des Nutzers möglich, gefälschte PROFINET-Gerätebeschreibungen (GSDML) werden als gültig signiert angezeigt, und es gibt eine Path-Traversal-Lücke. Betroffen sind CVE-2026-110935 und CVE-2026-110022 (CVSS 8,4) sowie CVE-2026-110021 (CVSS 6,2). Für CVE-2026-110935 und CVE-2026-110022 nennt das Advisory einen lokalen Angriffsvektor (AV:L). Meine Empfehlung (nicht aus der Quelle): Bis zum Update Plug-ins nur aus vertrauenswürdigen Quellen installieren und GSDML-Dateien nur aus Herstellerquellen importieren. Meine Einschätzung (nicht aus der Quelle): Das trifft die Engineering-Rechner von Integratoren und Betreibern mit PLCnext-Steuerungen, also auch in der Wasserwirtschaft. Quelle: https://certvde.com/en/advisories/VDE-2026-121/

Relevanz: MITTEL

L-02 Zyxel GS1900: Zero-Day in Switches ausgenutzt, fast 1.000 Geräte kompromittiert, Zyxel hat eine Lücke im Web-Management der Switch-Serie GS1900 geschlossen (laut BleepingComputer CVE-2026-107441, Out-of-bounds Write). Angreifer konnten damit ohne Anmeldung per präparierter HTTP-Anfrage Befehle ausführen und haben Konfigurationsdateien, gehashte Root-Zugangsdaten und Netzinformationen abgegriffen. Laut GreyNoise sind 996 Geräte in 48 Ländern betroffen, ausgenutzt seit etwa 17. August. Zyxel führt die Lücke als eigene Schwachstelle, weil der Exploit zusätzlich fehlende Längenprüfungen der HTTP-Parameter ausnutzt. Ob der Exploit gezielt gebaut wurde, um die Juni-Updates für CVE-2026-7273 zu umgehen, ist unklar. Betroffen sind zehn GS1900-Modelle; die Updates kamen am 22.10., das Advisory am 03.11. Wer GS1900 im eigenen Netz hat, auch in Anlagen- oder Stationsnetzen, sollte die Firmware vom 22.10. einspielen, die Management-Oberfläche nur aus einem Verwaltungsnetz erreichbar machen und die Zugangsdaten der Switches ändern (CC2 Defensible Architecture). Quelle: https://www.bleepingcomputer.com/news/security/zyxel-fixes-zero-day-exploited-to-hack-nearly-1-000-network-switches/

Relevanz: HOCH

L-03 Nach den Supermarkt-Angriffen: Kühllager des Blutspendedienstes EFS betroffen (02.11.), Betroffen sind Kühllager des staatlichen Blutspendeinstituts EFS; laut BleepingComputer war nicht EFS selbst das Ziel, sondern ein Kühl-Dienstleister. Unabhängig davon bestätigte Coolworld Rentals einen Vorfall mit seiner Fernüberwachungs-Software (laut Coolworld über eine Lücke in der Komponente eines Drittanbieters); ob Coolworld der Dienstleister der EFS ist, ist nicht bestätigt, EFS nennt ihn nicht. In drei Einrichtungen wurden Temperatur- und Abtau-Grenzwerte auf extrem hohe Werte gestellt. Laut EFS gingen keine Blutprodukte verloren, EFS arbeitet mit der ANSSI und dem Gesundheitsministerium zusammen. Ob die Täter dieselbe Methode wie bei den Supermarkt-Angriffen genutzt haben, ist nicht bestätigt. Für DACH zeigt der Fall, dass Fernüberwachung und Fernzugriff von Dienstleistern auch Kühlketten in Kliniken, Pharma und Lebensmitteln treffen können (CC4 Secure Remote Access). Quelle: https://www.bleepingcomputer.com/news/security/cyberattack-disrupts-blood-storage-refrigeration-systems-in-france/

Relevanz: HOCH

L-04 Barracuda Email Security Gateway & Co.: Lückenkette führt zu Root-Rechten, Zwei Lücken: CVE-2026-116606 (CVSS 9,3, Authentication Bypass, nur ESG) und CVE-2026-111560 (CVSS 8,6, Command Injection in der Zeitzonen-Einstellung). Die zweite trifft auch Load Balancer ADC, Message Archiver, WAF, WAF Control Center und Web Security Gateway. Patches gibt es; zu einer Ausnutzung machen weder Barracuda noch Mandiant eine Angabe. Unklar ist, ob die ESG-Lücke eine Anmeldung voraussetzt: Mandiant sagt, sie geht ohne Anmeldung. Barracuda verlangt im Advisory für beide Lücken Admin-Zugang, nennt CVE-2026-116606 aber zugleich „pre-authentication“. Quelle: https://www.securityweek.com/barracuda-email-security-gateway-authentication-bypass-opens-path-to-root/

Relevanz: MITTEL

L-05 SonicWall GMS: Zwei Lücken, es kommt kein Patch mehr (End of Life), CVE-2026-109593 (Dateien auslesen ohne Anmeldung) und CVE-2026-109594 (SQL Injection) betreffen GMS 9.5.2 und älter. GMS wird nicht mehr gepflegt, SonicWall rät zum Umstieg auf NSM. Zu einer Ausnutzung macht die Quelle keine Angabe. Wer seine SonicWall-Firewalls zentral über GMS verwaltet, sollte die Konsole abschotten und den Umzug planen. Quelle: https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-unpatched-flaws-in-end-of-life-gms-software/

Relevanz: MITTEL

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