OT-CYBER.DE

WEEKLY REPORT

OT-Cyber Situation Report All OT sectors

Edition CW 46/2026 · All OT sectors in DACH

Audience	Operators of plants and machines, critical infrastructure (KRITIS) and industry in Germany, Austria and Switzerland (DACH)
Reporting period	6 November 2026 to 13 November 2026
Version	1.0
Date	13 November 2026
Author	Maximilian Gilg, OT-Cyber.de
Classification	TLP:CLEAR, public sources only
Language	English edition of the German weekly report

This report summarises publicly available information. The relevance rating refers to operators of plants and machines in Germany, Austria and Switzerland. Dates are given as DD.MM. as in the sources.

Executive summary

In the reporting period (06.11. to 13.11.) the focus was on two topics: refrigeration systems and remote maintenance access. According to BleepingComputer (09.11.), France attributes the October attacks on Danfoss refrigeration controllers in around 700 targeted stores to a unit close to Iran's Revolutionary Guards. The later wave in November in six European countries has not been attributed. Our assessment: devices from these manufacturers are probably in use in DACH as well, so refrigeration equipment with remote maintenance belongs in the OT asset inventory.

The second construction site is remote access. On 10.11., MB connect line published two PHP vulnerabilities in the remote maintenance portal mbCONNECT24 via CERT@VDE (remote code execution without authentication, CVSS 3.1: 9.8 and 8.1). CISA lists a SonicWall SSL VPN vulnerability as actively exploited since 06.11. Siemens has no fix yet for the WinCC Graphics Designer. For OpenSSH on Linux systems with musl libc and without PAM, the fix is in OpenSSH 10.6p2. If you only manage one thing this week: patch remote maintenance portals and VPN gateways, and disconnect refrigeration controllers from the internet.

OVERALL ASSESSMENT · THREAT LEVEL ELEVATED

The threat level is elevated: France attributes the October attacks on refrigeration systems in French stores to a state actor, and the remote maintenance portal mbCONNECT24 has a critical vulnerability that needs no authentication. Secure remote access (CC4) and shielding reachable refrigeration controllers have priority.

Recommendation to management

This week, order an inventory of all remote maintenance access, including access by refrigeration contractors and machine builders, and have the patch level confirmed to you by the end of the month. In our assessment, service provider access is currently the most likely way in.

Trends

• Refrigeration is becoming a regular OT target: after the attacks in France, the attribution of the October attacks and the US fact sheet (05.11.), the focus is now on devices that in our assessment are also installed in DACH plants.

• A single PHP vulnerability (CVE-2026-109618) reaches several products through third-party components, with very different severity.

• Remote maintenance portals and VPN gateways remain the most important initial access into OT, this week with vulnerabilities at MB connect line and SonicWall.

• Embedded Linux in edge devices brings vulnerabilities from the IT world into the plant, and the patch depends on the manufacturer (OpenSSH SSHole).

Situation overview

ID	Item	Relevance	Source
L-01	MB connect line mbCONNECT24: remote code execution without authentication through bundled PHP (VDE-2026-128, CVSS 9.8)	**CRITICAL**	MB connect line, coordinated by CERT@VDE, 10.11.

ID	Item	Relevance	Source
L-02	Refrigeration attacks: France holds the IRGC-linked unit "Shahid Kaveh" responsible	**HIGH**	BleepingComputer, 09.11.
L-03	SonicWall SonicOS SSL VPN: CVE-2026-19868 actively exploited (CISA KEV)	**HIGH**	CISA, 06.11.
L-04	OpenSSH "SSHole": login without a valid password on Linux with musl libc without PAM (fixed in OpenSSH 10.6p2)	**HIGH**	OpenSSH (oss-security) / SecurityWeek, 06.11.
L-05	Siemens SIMATIC WinCC Graphics Designer: code execution through a crafted file, no fix yet (SSA-979641)	**MEDIUM**	Siemens ProductCERT, 10.11.

Exposed OT systems (Shodan, aggregated)

Status: 2026-11-13

We count services of typical OT protocols that are reachable from the internet. The numbers indicate attack surface, they do not prove a vulnerability. No individual systems are named. Siemens S7 = port 102 (all ISO-TSAP services, not only genuine S7 controllers), OPC UA = default port 4840.

Region	Total	Top protocols
Germany	139840	DNP3: 31446, OMRON FINS: 26419, ProConOS: 15503, Siemens S7: 7574, OPC UA: 4952
Austria	4663	HMI/VNC: 1007, DNP3: 959, Niagara Fox: 456, Siemens S7: 381, OPC UA: 149
Bavaria (Munich)	1525	OMRON FINS: 849, HMI/VNC: 200, DNP3: 183, Siemens S7: 28, OPC UA: 24
Salzburg	29	HMI/VNC: 8, Niagara Fox: 7, BACnet: 5, Siemens S7: 1, OPC UA: 1
Tyrol (Innsbruck)	41	HMI/VNC: 11, DNP3: 9, Niagara Fox: 6, Siemens S7: 2, OPC UA: 1

Items in detail

L-01 MB connect line mbCONNECT24: remote code execution without authentication through bundled PHP (VDE-2026-128, CVSS 9.8)

CRITICAL MB connect line, coordinated by CERT@VDE, 10.11. · Where: Remote maintenance portal of machine and plant builders · Deadline: immediately

What is new: mbCONNECT24 and mymbCONNECT24 from version 2.0.0 and before 2.21.6 contain a PHP with CVE-2026-109618 (CVSS 3.1: 9.8) and CVE-2026-109619 (CVSS 3.1: 8.1). According to the advisory, both vulnerabilities can lead to remote code execution without authentication. The fix is in version 2.21.6. The advisory does not report exploitation.

Why it matters: Remote maintenance connections to many machines and plants run through such a portal at the same time. Whoever takes over the portal gains initial access to all connected plants. In our experience, many operators do not run the portal themselves; it runs at the machine builder.

Recommendation: Update self-hosted instances to 2.21.6 immediately. For hosted instances, ask the machine builder in writing for the patch level and date, and until then only establish connections when needed.

Source: https://certvde.com/en/advisories/VDE-2026-128/ ✓ checked

L-02 Refrigeration attacks: France holds the IRGC-linked unit "Shahid Kaveh" responsible

HIGH BleepingComputer, 09.11. · Where: Refrigeration in retail, food production and hospitals · Deadline: 1 week

What is new: According to BleepingComputer, France attributes the October attacks on refrigeration systems in around 700 targeted supermarkets and other stores to the Shahid Kaveh unit, which is close to Iran's Revolutionary Guards. Compromised Danfoss refrigeration controllers were used, and there were at least 15 fires. France wants to propose new EU sanctions. The later wave in November with more than 115 stores in six European countries has not been attributed.

Why it matters: This attributes the October attacks in France to a state, but not the November wave. Our assessment for operators in DACH: the same device types are in use here, and an EU sanctions debate can trigger further attacks.

Recommendation: For refrigeration and cooling systems, define who shuts down in an emergency and how operation continues without remote control (CC1). Set plausibility limits with alarms for setpoints.

Source: https://www.bleepingcomputer.com/news/security/france-blames-iranian-hackers-for-supermarket-attacks-that-sparked-fires/ ✓ checked

L-03 SonicWall SonicOS SSL VPN: CVE-2026-19868 actively exploited (CISA KEV)

HIGH CISA, 06.11. · Where: VPN gateway for remote maintenance and remote access · Deadline: immediately

What is new: CISA has added CVE-2026-19868 in SonicOS SSLVPN (use of single-factor authentication) to the KEV catalog because there is evidence of active exploitation.

Why it matters: At smaller municipal utilities, special-purpose associations and mid-sized companies, SonicWall firewalls are often the only gate into OT. A hijacked VPN account is direct initial access into the plant network.

Recommendation: Read the vendor advisory for CVE-2026-19868 and patch, enforce phishing-resistant MFA on the SSL VPN and check the VPN logs of recent weeks for logins at unusual times or from foreign countries.

Source: https://www.cisa.gov/news-events/alerts/2026/11/06/cisa-adds-one-known-exploited-vulnerability-catalog ✓ checked

L-04 OpenSSH "SSHole": login without a valid password on Linux with musl libc without PAM (fixed in OpenSSH 10.6p2)

HIGH OpenSSH (oss-security) / SecurityWeek, 06.11. · Where: Routers, gateways and edge devices on OpenWrt, Buildroot or Yocto · Deadline: 2 weeks

What is new: The vulnerability affects sshd on Linux systems with musl libc and PAM switched off, according to SecurityWeek among others Alpine, OpenWrt, Buildroot and Yocto. With a password of 257 to 1,024 characters a login is possible under certain conditions. It is fixed in OpenSSH 10.6p2, and Alpine called for patching on 05.11. According to Detectify, no exploitation is known yet, but the details are public.

Why it matters: Many industrial routers, telecontrol gateways and edge devices are built on exactly these embedded distributions. Only the manufacturer can say whether a product is affected, so the fix often arrives weeks later here.

Recommendation: Mark devices with SSH access based on embedded Linux in the asset inventory and ask the manufacturers whether they are affected. Until the update, switch off password logins or allow SSH only from the management network.

Source: https://www.securityweek.com/openssh-rushes-patches-for-sshole-authentication-bypass/ ✓ checked

L-05 Siemens SIMATIC WinCC Graphics Designer: code execution through a crafted file, no fix yet (SSA-979641)

MEDIUM Siemens ProductCERT, 10.11. · Where: Engineering stations and control systems with WinCC V7.5 to V8.1 · Deadline: ongoing

What is new: CVE-2026-59082 (CVSS 3.1: 7.8) affects the Graphics Designer in WinCC V7.5, V8.0 and V8.1, all versions in each case. Opening a crafted file can execute code. There is no fix yet; Siemens is preparing one.

Why it matters: WinCC is widespread in DACH industry and at utilities. Project files often arrive by e-mail or USB stick from the system integrator. A single manipulated file can therefore take over the engineering station.

Recommendation: Open external project files only after checking them and only from known sources. Separate engineering stations from the office network (CC2) and schedule the fix as soon as Siemens publishes it.

Source: https://cert-portal.siemens.com/productcert/html/ssa-979641.html ✓ checked

Recommendations

No.	Measure	Ref.	Priority	Timeframe
M-01	Have remote maintenance portals such as mbCONNECT24 patched by the service provider and enable connections only when needed [CC4 Secure Remote Access]	L-01	HIGH	immediately
M-02	Create and exercise an emergency plan for refrigeration and cooling systems with a shutdown path and manual operation [CC1 ICS Incident Response]	L-02	MEDIUM	0 to 3 months
M-03	Risk-based vulnerability management for edge devices and routers: follow up manufacturer inquiries about OpenSSH [CC5 Risk-Based Vulnerability Management]	L-04	MEDIUM	0 to 3 months
M-04	Segment engineering stations (WinCC) and route incoming files through a check station [CC2 Defensible Architecture]	L-05	LOW	3 to 6 months

Questions for your next team meeting

1. Which refrigeration and cooling controllers do we have, and who has remote access to them?

2. Do our machine builders run remote maintenance portals such as mbCONNECT24, and when will they be patched?

3. Is our VPN gateway protected with phishing-resistant MFA, and who reviews the logs?

4. Which edge devices and routers have SSH open, and what do the manufacturers say about SSHole (OpenSSH 10.6p2)?

5. How do we open WinCC project files from the integrator, and is there a check station for this?

Actions for this week

1. Search the asset inventory for refrigeration controllers, check whether they are reachable from the internet and ask the manufacturer for the firmware status.

2. Ask all machine and plant builders in writing for the patch level of mbCONNECT24 (2.21.6).

3. Patch the SonicWall SSL VPN and check the VPN logs of the last 30 days for unusual logins.

4. Define an emergency mode without remote control for refrigeration and cooling systems and agree it with the service provider.

NOTE ON SOURCES

We checked the primary sources CISA, CERT@VDE and Siemens as well as the OpenSSH announcement on oss-security (05.11., without a CVE identifier; a CVE number mentioned in the press could not be confirmed and is therefore left out). The French attribution is only documented via BleepingComputer; we did not find the statement of the foreign ministry itself. Not included because not sufficiently documented: a blog report that the BSI had confirmed incidents at supermarkets in Germany, the fixed versions for SonicWall CVE-2026-19868, and concrete OT incidents in Austria and Switzerland in calendar week 46 (none found). The US fact sheet on refrigeration systems of 05.11. predates the reporting period. All source links were opened and checked for content automatically on 13.11.2026. This English edition is a translation of the German weekly report of the same date; items that did not pass the source check are left out here as well.

OT-Cyber.de, Rosenheim (Bavaria). Questions about this report or support for your plants: ot-cyber.de/en