Alleged Attack on French Blood Establishment (EFS)

Nov 04, 2026

WHITE

View Alert

On November 4, 2026, reports on the alleged attack on the French Blood Establishment (EFS) started circulating in French news outlets.

While the alleged attack has been reported in the news outlets, at this time no relevant government websites have published an official press release to substantiate it.

This alert is issued for situational awareness, highlighting how recent operational technology (OT) attacks against specific refrigeration brands directly intersect with emerging threats to the health sector

Additional Info

These reports claim that unknown threat actor targeted Coolworld, a maintenance contractor for France's national blood agency (EFS), during the night of November 1st to 2nd, attempting to heat deep-freeze units storing donor blood samples.

However, allegedly, the overnight temperature spike was spotted in time, allowing staff to intervene before the products were compromised. The reports also claim the France's Health Ministry confirmed that because the attack was promptly caught, it caused no operational impact on blood supplies or transfusion services; however, no official report on the Ministry's website has been released at this time.

Although official sources have not yet validated these reports with official press releases, the threat remains highly relevant to the health sector.

To counter the ongoing wave of refrigeration attacks and related cyber campaigns targeting operational technology (OT), Health-ISAC urges members to implement the following safeguards:

- Scan and shut down all public-facing IP ports for refrigeration controllers, BMS supervisors, and serial-to-Ethernet gateways (e.g., Dixell, Carel, Emerson).
- Isolate all refrigeration, medical gas, and telemetry devices on dedicated VLANs completely segregated from general hospital IT and guest Wi-Fi, blocking cross-traffic by default.
- Identify and isolate third-party 4G/5G gateways or vendor modems attached to chillers, forcing their traffic through managed enterprise firewalls or private APNs.
- Replace persistent vendor VPNs with Just-In-Time (JIT) privileged access requiring multi-factor authentication (MFA) that automatically expires after maintenance windows.
- Funnel all external technician sessions through an intermediary jump server that logs commands and records sessions, banning unmonitored tools like TeamViewer or AnyDesk.
- Place independent, hard-wired mechanical thermostats or thermal relays in series with heating and compressor circuits to physically cut power if limits are exceeded, regardless of software overrides.
- Replace generic manufacturer credentials (admin/admin, 1234) across all local controller displays, supervisory web servers, and Modbus/BACnet bridges with unique, complex passwords.
- Never rely solely on the vendor's own software for alarms. Use secondary, isolated IoT sensors (e.g., LoRaWAN) that report directly to internal security and clinical teams.
- Configure alarms to trigger immediately whenever operating parameters, defrost cycles, or target temperatures are modified, especially outside standard change-control hours.

- Train on-site biomedical and facility staff to engage physical mechanical bypasses to keep units running offline, and maintain offline backups of all controller configurations.

<hr size=1 width="100%" align=center>

Alert Id	51946e56
Category	Threat Bulletins
Tags	Blood Supply, Operational technology (OT), Cyberattacks

Sources

https://www.lemonde.fr/en/france/article/2026/11/04/new-cyberattack-targets-french-blood-banks_6771517_7.html
https://www.cyberattaque.org/cyberattaque-contre-lefs-des-hackers-sattaquent-aux-reserves-de-plasma-sanguin/
https://www.aa.com.tr/en/science-technology/french-blood-storage-facilities-targeted-in-cyberattack-report/4110658
https://www.telegraph.co.uk/world-news/2026/11/04/hackers-hit-french-blood-bank/

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like | Dislike

Download the App
Available on iOS, Android and Web

Download on the App Store | Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a1a6758c92-3432a1f1-9156-476b-a99f-18fec79693db-000000%40email.amazonses.com.