FBI and CISA issue warning on cyberattacks against refrigeration systems



The FBI and CISA have warned of cyberattacks targeting refrigeration systems. The source text was unreadable, so details are not reproduced; operators should consult the original advisory.

- The FBI and CISA have jointly warned about cyberattacks aimed at refrigeration systems.
- The source text we received was corrupted, so technical details, affected products and timelines are not stated here.
- Refrigeration is operational technology that many food, pharmaceutical and logistics operators rely on.
- The original BleepingComputer report and the agencies' advisory should be reviewed directly.

What was reported

BleepingComputer reports that the FBI and CISA have warned of cyberattacks targeting refrigeration systems. The text supplied to us for this item was unreadable, so we cannot responsibly describe the attack methods, affected vendors, victims or recommended mitigations.

Why it matters

Cold-chain equipment is increasingly network-connected and often managed outside the core IT security programme. Organisations in food, healthcare, pharmaceuticals and logistics may depend on it for continuity, so a warning from two national agencies is worth a prompt internal check even before full details are reviewed.

What to do next

Read the original report and the agencies' advisory, then confirm with facilities and operations teams whether refrigeration or building-management systems are connected to any network, who maintains them, and how they are monitored. Apply the technical guidance from the advisory once verified, rather than relying on this summary.

What to do now

1. Read the original BleepingComputer report and the FBI/CISA advisory in full.
2. Inventory refrigeration and building-management systems and note which are network-connected.
3. Confirm with facilities teams and third-party maintainers who has remote access to these systems.
4. Check that these systems are covered by monitoring and incident response plans.
5. Apply the advisory's technical mitigations once verified against your environment.