It's Probably Nothing
by Sierra Echo Charlie

EDITION 02 / 14 OCTOBER 2026

Ivanti chain gets root on patched VPNs; fridge alert grows

CERT-FR adds Copeland and Dixell kit, Ledger explains its LTE implant, and LiteLLM gets a fix.

5 stories / Listen online - 4:25

THE TAKEAWAY

Today has a VPN zero-day chain that Ivanti's own integrity tool can't see, and a supermarket fridge campaign that now involves more than one vendor. There's also an AI worm forecast and a hardware wallet that phoned home over LTE.

01 / THE BRIEF

Ivanti Connect Secure chain reached root on a patched box, and one link is still unfixed

Ivanti has disclosed CVE-2026-104935, an authentication bypass in Connect Secure, and says it knows of limited exploitation. CISA added it to KEV on 13 October. Volexity's write-up is the uncomfortable part. It says an actor it tracks as UTA0576 chained the bypass with an RCE (both covered by that CVE) and a privilege escalation. That gave unauthenticated root on an appliance that was fully patched at the time, running 22.8R2.4. Volexity dates the activity from 3 October, and Defused told BleepingComputer it saw first signs on 1 October.

The privilege escalation, which is in how the dsinvoked broker trusts DSCache data, isn't fixed yet. Ivanti plans a fix in the coming weeks. The exploit patches library code in memory only and restores the config data it changes, so the Integrity Checker Tool sees nothing, and Volexity found no web shell. The actor then went after AD credentials, LAPS passwords and BitLocker recovery keys, and deleted entries from the debug and Linux audit logs.

Ivanti's advice to run the ICT regularly sits a bit awkwardly next to that. A clean scan doesn't clear you here.

WORTH ASKING

SecurityWeek lists fixes in 22.8R2.5, 25.1.1.2, 25.1.3.0 and 25.1.3.1. If you run ICS, patch, but treat 'were we hit since early October?' as a forensics question. Personally, I'd be thinking about the secrets it was after, too.

QUALIFICATIONS

Volexity's chain findings describe one actor. 'Limited exploitation' is Ivanti's description. BleepingComputer says Shadowserver tracks more than 5,500 exposed ICS instances, but it's unknown how many are honeypots or already secured.

SOURCES

Ivanti Connect Secure Authentication Bypass Exploited for Remote Command Execution (Mallory) - Reporting / context

A Series of Unauthenticated Events: Chained Exploitation of Ivanti Connect Secure Zero-Days - Primary source

CISA Known Exploited Vulnerabilities catalogue (JSON feed) - Primary source

Ivanti warns of Connect Secure zero-day exploited in attacks - Reporting / context

Ivanti Zero-Day Chain Gave Attackers Root Access to Fully Patched VPN - Reporting / context

02 / THE BRIEF

CERT-FR says fridge controller compromises are 'numerous' and adds Copeland and Dixell XWEB

Quick recap: this is the French supermarket refrigeration attack from yesterday. CERT-FR's alert CERTFR-2026-ALE-012 now says it knows of numerous compromises of Danfoss AK-SM and AK-SC remote controllers. Its 13 October revision adds Copeland XWEB and Dixell XWEB to the targeted kit. CERT-FR thinks campaigns are probably still under way. It also warns that an exposed end-of-life unit is very likely to be compromised again, and that a factory reset alone doesn't help. Cybernews, citing La Dépêche, reports that an E.Leclerc near Albi running Dixell equipment had a major refrigeration failure early on Tuesday.

So this has stopped being one vendor's legacy firmware problem. It's now about internet-exposed refrigeration controllers in general. CERT-FR's advice is pleasingly concrete: remove internet exposure, check the config (especially defrost schedules), and restore access only through a VPN. Filtering to contractor IPs is acceptable only as a stopgap. It also says to check your insurance terms before cutting data feeds to the refrigeration contractor, which is exactly the kind of detail only real incident response produces.

WORTH ASKING

If you have AK-SM, AK-SC or XWEB units anywhere near a public IP, this is worth chasing down this week.

QUALIFICATIONS

CERT-FR names no victims, attacker or CVE, and the access method is unconfirmed. Exposure counts differ: Cybersecuritynews found 4,980 Danfoss hosts on Shodan, more than half of them in France, while Cybernews cites about 2,900. A claim that the password was simply the current date is unverified.

SOURCES

Cyberattack Manipulates Refrigeration at French Supermarkets, Destroying Fresh Stock (Mallory) - Reporting / context

Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération - CERT-FR (CERTFR-2026-ALE-012) - Primary source

Frigos de supermarchés sabotés : les cyberattaques qui vident les rayons - Reporting / context

Danfoss Refrigeration Hack Update - 4,980 Hosts Found Exposed to Internet - Reporting / context

Food safety fears grow as Copeland is named as second fridge supplier hit in supermarket hacking spree - Reporting / context

03 / THE BRIEF

Anthropic thinks small models may soon be able to worm across cheap IoT

Anthropic's Frontier Red Team says small models may be months away from self-replicating on commodity devices such as off-brand Android TV boxes. In its tests, a 9B model got inference running on 8 of the 9 hardware types. In a deliberately simplified worm test, spreading over unauthenticated ADB across 8 GCP nodes running an Android 15 emulator, GLM-5.2 and stronger models managed end-to-end replication. Models of 30B and under can do many of the steps but fumble chaining them. Anthropic's rough trend fit puts small models at GLM-5.2's level by the end of 2026.

This is a forecast, not an outbreak, and Anthropic itself calls the result an upper bound, because the exploit step was trivial. But a slow worm with a doubling time of days and no central off switch is a properly annoying shape of problem. The defence is the boring one: don't leave ADB open to the network.

SOURCES

Anthropic Tests Highlight Potential for Self-Replicating AI Worms on IoT Devices (Mallory) - Reporting / context

AI models may be capable of self-replicating without access to a datacenter - Primary source

Small AI Models May Soon Be Able to Self-Replicate on IoT Devices, Anthropic Warns - Reporting / context

04 / THE BRIEF

Ledger: CryptoBilis-sold wallets read the seed phrase off the screen and sent it over LTE

According to The Record, Ledger said on Tuesday that devices sold through Southeast Asian reseller CryptoBilis had hidden implants that read the display during setup. They picked out the 24-word recovery phrase and sent it out over LTE using an embedded eSIM. Funds were drained on 9 October. Ledger says it hasn't confirmed total losses. SecurityWeek's headline links a US$86 million heist to the implant. The Defiant notes that Genuine Check can't rule out tampering that leaves the secure chip intact, which is rather the point of the attack.

WORTH ASKING

Ledger says CryptoBilis buyers shouldn't set up unused devices and should contact support. Anyone who has already set one up should move funds to a new signer with a new recovery phrase.

QUALIFICATIONS

Ledger's posts weren't read directly. Claims that tampered devices came through other channels are unverified.

SOURCES

Ledger-CryptoBilis Theft Losses Near $93 Million as Funds Move to USDD and Tornado Cash (Mallory) - Reporting / context

Ledger says hardware implant in cryptocurrency wallets stole recovery phrases - Reporting / context

Ledger Says CryptoBilis-Sold Wallet Implants Transmit Recovery Phrases Over LTE - Reporting / context

$86 Million Crypto Heist Linked to Ledger Signer Hardware Implant - Reporting / context

05 / THE BRIEF

LiteLLM bugs let a read-only user take over the gateway and its provider keys

Check Point Research disclosed CVE-2026-35029 and CVE-2026-59823 in LiteLLM. IT Security Guru says the first is a missing PROXY_ADMIN check on /config/update, combined with loosely checked dashboard session tokens. Check Point says it let even read-only users take over the gateway, and it demonstrated file access and RCE in a test environment. The second let authenticated users point gateway requests at their own server and collect AI provider API keys. Both are fixed in 1.83.9 and later.

An AI gateway is essentially a vault of API keys with a dashboard bolted on, so a read-only role meaning 'admin, actually' is not ideal.

WORTH ASKING

If you run LiteLLM below 1.83.9, it's worth upgrading.

QUALIFICATIONS

No in-the-wild exploitation has been reported, and the CVSS scores weren't verified.

SOURCES

LiteLLM Flaws Enable Gateway Takeover, Remote Code Execution and API-Key Theft (Mallory) - Reporting / context

Check Point Research Discovers High Risk Vulnerabilities in LiteLLM, One of the Most Widely Used LLM Gateways - Primary source

LiteLLM flaws let low-privileged users hijack AI gateway and steal provider keys - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.