Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

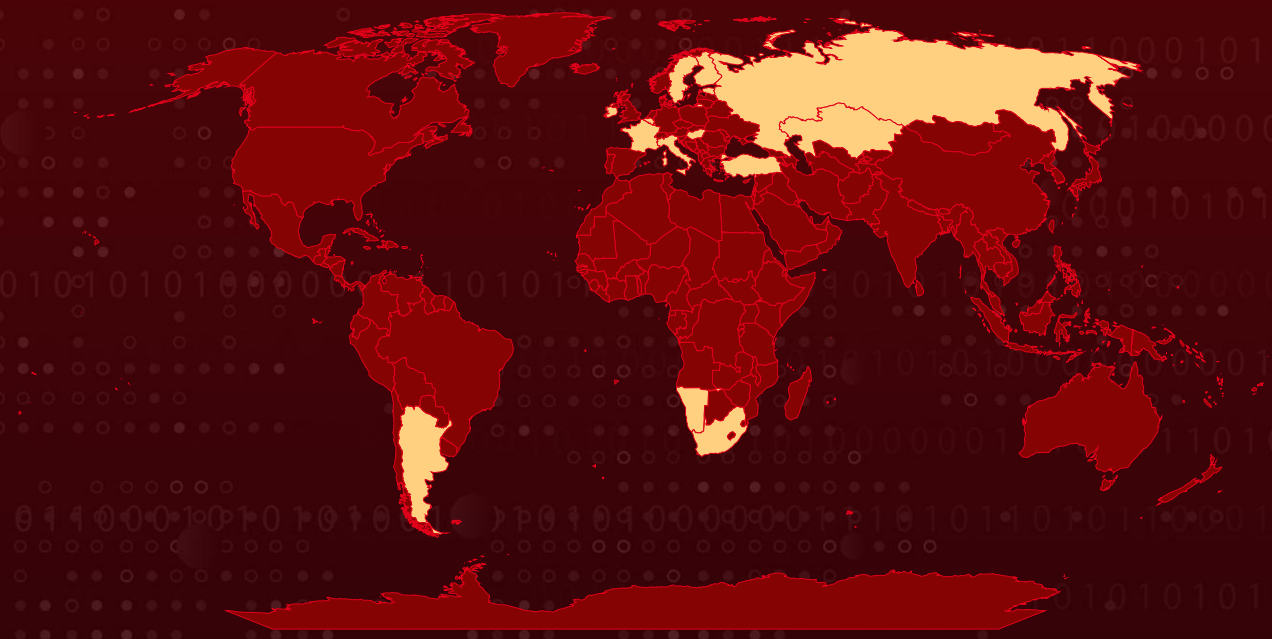
Refrigerator Botnet Hijacks Exposed Copeland XWEB Controllers

Date of Publication	Admiralty Code	TA Number
November 12, 2026	A1	TA2026336

Summary

First Seen: November 2 2026
Targeted Regions: Argentina, Italy, Russia, Kazakhstan, Belgium, Turkey, Hungary, France, Namibia, Trinidad and Tobago, South Africa, Sweden, Finland, Ireland, Luxembourg, Estonia
Targeted Platforms: Embedded Linux (Copeland XWEB firmware)
Targeted Products: Copeland (Dixell) XWEB 300D PRO, XWEB 500D PRO, XWEB 500B PRO, XWEB EVO
Targeted Industries: Retail, Food & Beverage, Cold-Chain Logistics, Hospitality
Malware: Refrigerator Botnet
Attack: An unattributed operator is quietly taking over internet-facing Copeland (Dixell) XWEB refrigeration controllers left on outdated firmware (1.12.1 and prior), most likely by bypassing their login through CVE-2026-25085. Rather than disrupting cooling, the operator turns these store and cold-chain devices into hidden infrastructure, relaying VPN and proxy traffic and sending spam from what appear to be ordinary business networks across Europe, the Americas, Africa and Central Asia. Exposed XWEB units were also among the controllers abused in recent European incidents where fridge and freezer settings were changed and alarms silenced, spoiling stock, although those incidents have not been linked to this botnet.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Targeted Non-Targeted

CVE

CVES	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-25085	Copeland XWEB Pro Authentication Bypass Vulnerability	Copeland XWEB Pro	✗	✗	✓
CVE-2026-21718	Copeland XWEB Pro Predictable Credentials Authentication Bypass Vulnerability	Copeland XWEB Pro	✗	✗	✓
CVE-2026-24663	Copeland XWEB Pro OS Command Injection Vulnerability	Copeland XWEB Pro	✗	✗	✓

Attack Details

#1

Across supermarkets, cold stores and medical storage sites, Copeland XWEB supervisory controllers quietly run the refrigeration that keeps stock safe. Many of them sit directly on the internet, with their web interface open on ports 8015 and 443. Units still on firmware 1.12.1 or earlier carry a cluster of 23 publicly disclosed flaws that were fixed in version 1.13. An unattributed operator is now sweeping up those unpatched devices and wiring them into a botnet.

#2

The most likely way in is CVE-2026-25085, an authentication bypass in the controller's Lua login routine. When it receives an unrecognized login type, it returns an empty result that the web router accepts as a successful login, so the attacker gets in without a password. CVE-2026-21718 offers a second route, letting anyone calculate the daily administrator password from a hard-coded seed, the device MAC address and the date, all of which leak through unauthenticated pages. On some sites no exploit was needed at all, because controllers were still running with their default administrator credentials.

#3

Once inside, the attacker can push shell commands through any of 19 command injection flaws, where user input is handed straight to Lua system calls without sanitization. One of them, CVE-2026-24663, needs no login at all. Because the affected services run with elevated privileges, the attacker ends up with root control of the embedded Linux controller. The derived administrator password can also switch on SSH or the browser-based Shellinabox console for hands-on access.

#4

Rather than breaking the hijacked units, the operator puts them to work. One controller in Namibia became an OpenVPN/IPsec tunnel gateway carrying about 71% of observed flows, including roughly 1.24 million sessions to a single endpoint in South Africa on port 443. Another, in Trinidad and Tobago, became a residential-proxy exit, with 99.6% of its traffic originating from the device and fanning out to 10,643 peers in 17 hours over WireGuard, STUN, MQTT and DNS. To anyone on the receiving end, that traffic appears to come from an ordinary retail network.

#5

A separate cluster of nine IP addresses in Argentina, Italy, Russia, Kazakhstan, Belgium, Turkey, Hungary and France acts as outbound-only spam senders, mailing out on ports 25, 465 and 587 while receiving none, and only three of these IPs are confirmed XWEB controllers. Together they reached 1,041 mail targets, 508 of them hit by two or more nodes, and the three busiest nodes share about 47% of their targets. That overlap is the strongest sign of a single coordinated operator. Two endpoints shared by the spam nodes, on ports 993 and 2525, may serve as command and control, though that link is weak.

#6

The controller is also a bridge into the refrigeration hardware behind it. With root access over SSH, an attacker can map the Modbus registers of serially connected field controllers, set displayed temperatures anywhere from -50°C to 110°C, and switch off fans, compressors, defrost and lighting while the display still shows normal readings. In one observed intrusion, two administrator sessions first read settings from 31 connected cases, freezers and cold rooms, then made 743 parameter writes within about half an hour. Setpoints were pushed to 110°C and 150°C, alarms were muted or set to extreme thresholds, keypads were locked and defrost cycles forced.

#7 No data theft has been reported; the damage comes from hijacked devices and, where settings are changed, spoiled stock. Since October 2026, waves of refrigeration tampering have hit supermarkets and medical cold storage across Europe, forcing units into defrost and heating some to as high as 50°C. Those incidents have not been tied to this botnet, and its operator remains unattributed. Many of the addresses linked to the botnet belong to compromised victim devices, not to attacker-owned infrastructure.

Recommendations

Upgrade Copeland XWEB Firmware to 1.13: Upgrade every XWEB 300D PRO, 500D PRO, 500B PRO and XWEB EVO unit on firmware 1.12.1 or earlier to version 1.13 or later, either from the Copeland software update page or directly on the device through SYSTEM, Updates, Network. Back up the configuration and logs first, and check after the update that alarms, sensors, defrost and cooling behave normally. Changing passwords alone does not close CVE-2026-21718 or CVE-2026-25085; only the firmware fix does.

Find and Close Exposed XWEB Interfaces: Scan your own public IP ranges for ports 8015 and 443 serving an XWEB login page, a TLS certificate naming "XWEB PRO" or "Dixell", or a page titled "XWEB EVO", and remove the port forwarding or public NAT rule behind each hit. Many of these devices were installed by refrigeration contractors, so check site routers and contractor-managed connections, not only the corporate perimeter.

Replace Default XWEB Administrator Credentials: Set a unique, strong Administrator password on every controller, since default credentials alone were enough for attackers to take over a live site. Do the change from a trusted workstation and record which contractor accounts still exist.

Block Outbound Mail and Tunnel Traffic from Controllers: Deny outbound connections on ports 25, 465, 587, 993 and 2525, along with OpenVPN, IPsec, WireGuard and proxy traffic, from any network segment that holds refrigeration controllers. A controller has no business sending mail or carrying VPN tunnels, so these rules break the botnet's main uses without affecting refrigeration.

Hunt for XWEB Hosts Sending Spam or Proxy Traffic: Look in firewall and NetFlow logs for any XWEB device that sends mail to many external servers with no inbound mail, carries large volumes of tunnel or proxy sessions, or talks to 46[.]255[.]231[.]42 on port 993 or 143[.]244[.]202[.]96 on port 2525. Any hit should be treated as a compromised controller and taken offline for rebuild.

Alert on Bulk Parameter Writes and Unsafe Setpoints: Feed XWEB event logs into monitoring and alert on more than about 20 parameter writes per minute from one account, writes to more than three devices within five minutes, setting reads right after login, setpoints or alarm thresholds outside a plausible range, keypad locks, alarm mutes, and defrost commands outside the schedule.

Audit Controllers Before Reconnecting Them: On any controller that was exposed, review setpoints, defrost schedules, alarm thresholds and delays, keypad lock status and user accounts against a known-good baseline. Confirm that SSH and Shellinabox are disabled unless you actually need them, and rebuild the device if anything looks unfamiliar.

Add Independent Temperature Alarms: Install temperature sensors and alerts that do not depend on the XWEB controller, because a compromised controller can show normal readings while fans and compressors are switched off. Train store staff to act when the controller display and the independent reading disagree.

Route Contractor Access Through a Managed VPN with MFA: Where refrigeration contractors need remote access, give it to them through an organization-managed VPN with MFA, named accounts and time-limited sessions, instead of a direct internet path to the controller.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	
Resource Development	T1584: Compromise Infrastructure	T1584.005: Botnet
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	T1078.001: Default Accounts
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Lateral Movement	T1021: Remote Services	T1021.004: SSH
Command and Control	T1572: Protocol Tunneling	
	T1090: Proxy	T1090.002: External Proxy
	T1071: Application Layer Protocol	T1071.003: Mail Protocols

Tactic	Technique	Sub-technique
Impact	T1496: Resource Hijacking	T1496.002: Bandwidth Hijacking
Discovery	T0861: Point & Tag Identification	
Impair Process Control	T0836: Modify Parameter	
Inhibit Response Function	T0878: Alarm Suppression	
Execution	T0855: Unauthorized Command Message	
Impact	T0831: Manipulation of Control	
	T0832: Manipulation of View	
	T0879: Damage to Property	

*Note: TTPs marked from the MITRE ATT&CK for ICS matrix.

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	197[.]188[.]223[.]161, 168[.]195[.]122[.]22, 181[.]192[.]79[.]179, 151[.]3[.]178[.]94, 213[.]221[.]44[.]60, 85[.]29[.]149[.]211, 78[.]21[.]151[.]21, 95[.]229[.]5[.]248, 178[.]244[.]215[.]186, 84[.]1[.]34[.]242, 90[.]0[.]156[.]128, 198[.]251[.]85[.]67, 85[.]137[.]52[.]63
IPv4:Port	160[.]19[.]119[.]226[:]443, 46[.]255[.]231[.]42[:]993, 143[.]244[.]202[.]96[:]2525
Hostname	VPS-97D1AF38, U6SFQPST

Recent Breaches

https://www.delhaize.be

https://www.carrefour.com

https://www.colruytgroup.com

https://www.ica.se

https://www.coop.se

https://www.kesko.fi

https://www.intermarche.pt

https://www.efs.sante.fr

Patch Links

https://webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate

https://webapps.copeland.com/Dixell/Pages/XWEB300D_500D_500_PRO

References

https://securityscorecard.com/blog/a-dish-served-lukewarm-the-refrigerator-botnet/

https://claroty.com/team82/research/chilling-discoveries-unpacking-vulnerabilities-in-copeland-xweb-pro-controllers

https://ransom-isac.org/blog/the-copeland-incident/

https://www.securityweek.com/over-100-european-stores-hit-as-supermarket-fridge-attacks-resume/

https://cybersecuritynews.com/iranian-hackers-supermarket-cyberattacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 12, 2026 • 10:40 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com