It's Probably Nothing
by Sierra Echo Charlie

EDITION 30 / 18 NOVEMBER 2026

Puppet joins KEV, and Java4Shell leaks early

Plus unpatched fridge controllers, offshore GPU rentals and a free CSAM classifier

4 stories / Listen online - 5:16

THE TAKEAWAY

Today's mix includes a confirmed-exploited bug in the thing that configures your fleet, a Java flaw that's mostly rumour so far, and some fridge controllers that took one researcher less than an hour to pick apart.

01 / THE BRIEF

Puppet Server report bug is now officially being exploited

On 17 November (US time), CISA added CVE-2026-115731 to its Known Exploited Vulnerabilities catalogue, with a 1 December due date. The flaw sits in Puppet Server's report processing. Any client with a CA-signed agent certificate can submit a report via PUT containing a crafted rich-data type and run code as the Puppet service user. Fixes landed from 4 November, and public proof-of-concept details are reportedly around. The KEV entry is the first agency confirmation of exploitation we've seen. CISA gives no attack detail and lists ransomware use as unknown.

The certificate requirement sounds reassuring until you think about autosigning. If your CA signs requests without strong verification, an unauthenticated attacker can simply ask for a certificate. OSG notes that code running as the service user isn't root by itself. Still, a Puppet server is a bad place for a stranger to be running code, given everything it configures. The companion bug, CVE-2026-115732, accepts certificates whose names extend or shorten an authorised hostname. In Puppet Enterprise, OSG says that could reach CA administration and remote command execution on managed nodes.

WORTH ASKING

According to OSG, the fixed versions are Puppet Enterprise 2023.8.13, 2025.12.1 and 2026.0.1; Puppet Core 8.22.1 and 9.1.3; and OpenVox Server/OpenVoxDB 8.18.0 and 9.2.0. If patching has to wait, OSG suggests turning off unverified autosigning first and keeping management endpoints restricted to trusted agent networks.

QUALIFICATIONS

Perforce's own advisory was unavailable when checked, so the version list comes from OSG and Puppet's notice.

SOURCES

CISA Known Exploited Vulnerabilities catalogue (CSV) - Primary source

OSG-SEC-2026-11-06 CRITICAL- Puppet Server vulnerabilities- CVE-2026-115731 and CVE-2026-115732 - Reporting / context

Security Notice: Important Action Recommended for all Puppet Users - Primary source

02 / THE BRIEF

Java4Shell: big name, small amount of confirmed detail

A reported pre-authentication memory-corruption flaw in OpenJDK, CVE-2026-114938, leaked on Oracle's 17 November Java patch day. Calif says on X that it found and reported the bug, that it leaked, and that it will publish details after Oracle patches. The reported CVSS 4.0 score is 9.2, reportedly affecting OpenJDK 17.0.6 onward. However, the CVE record is still reserved and those details are unconfirmed. In Mallory's summary, Oligo describes an integer underflow in the AVX-512 Base64 decoder, where a crafted 65-byte input causes a 62-byte heap overflow. Datadog calls it an out-of-bounds write and says it's still investigating.

Oracle's advance notice covers 11 Java SE flaws, all remotely exploitable without authentication, with a maximum CVSS 3.1 score of 8.1. There's no evidence yet that Java4Shell is one of them. According to Oligo, real exposure depends on the build, the hardware path and whether attacker input reaches that decoder at all. That's a lot of conditions for something carrying a 4Shell suffix. No source shows exploitation in the wild.

WORTH ASKING

This is a decent excuse to find out where your Java runtimes actually live. The details can be checked once Calif publishes.

QUALIFICATIONS

The affected range, mechanism and fix mapping are all reported rather than vendor-confirmed.

SOURCES

Oracle to Patch 11 Java Flaws Today as Critical OpenJDK RCE (CVE-2026-114938) Report Emerges - Reporting / context

Java4Shell: Remote Code Execution in OpenJDK (CVE-2026-114938) - Reporting / context

Reported Java4Shell Flaw in OpenJDK Base64 Decoder Raises Remote Code Execution Risk - Reporting / context

03 / THE BRIEF

Catching up: six unpatched pre-auth holes in Danfoss fridge controllers

This one first surfaced around 10 November and circulated through 16 November. Carlo Meijer of Midnight Blue reported six pre-authentication flaws in Danfoss AK-SM800A refrigeration controllers on firmware 5.3.2. He found them in under an hour of manual review. Five are in unauthenticated web handlers running as root, and the researchers ran root code on firmware 3.3.0. The sixth is in the gateway that enforces Strict mode. It crashed the gateway in emulation, and the researchers think it could become code execution. There's no patch and no CVE. The researchers say 5.4.0 doesn't fix the flaws, and BSI corrected an earlier statement to say it can't rule out 5.4.0 being affected. The devices also lack secure boot and stack canaries, which the researchers say could allow persistence that survives a reset.

These are the controllers caught up in the supermarket refrigeration attacks we've been following. Even so, BSI has no information about exploitation of these six flaws, and nobody links them to those attacks. Belgium's CCB says to remove direct internet exposure now, including via 4G/5G modems. Danfoss's own guide already says the device shouldn't be directly internet-reachable on any version. Danfoss didn't respond to The Register.

QUALIFICATIONS

Midnight Blue's write-up and the agency advisories weren't read directly.

SOURCES

Six Unpatched Danfoss Refrigeration Controller Flaws Could Allow Remote Takeover Without Login - Reporting / context

'Not rocket surgery' claims researcher who found six Danfoss fridge controller zero-days in under an hour - Reporting / context

Six Pre-Authentication RCE Flaws Expose Danfoss Refrigeration Controllers to Takeover - Reporting / context

04 / THE BRIEF

US moves to stop renting GPUs offshore to restricted customers

On 16 November, BIS issued an immediately effective rule restricting remote access to advanced US chips through third-country data centres. Overseas providers serving companies in countries such as China, Russia, Iran and Cuba must identify end users. They also need a licence to give remote access to companies headquartered in China or other restricted destinations, and existing providers get 90 days. Chip sales to Indonesia, Malaysia, Singapore, Thailand and Brazil now face case-by-case licensing as diversion risks. The rule also rescinds the regulations implementing the Biden-era AI Diffusion Rule, and comments are due within 60 days.

Singapore and Malaysia are now explicitly in scope, which pulls a fair chunk of regional cloud capacity into US export compliance.

QUALIFICATIONS

The rule text wasn't read; details come from AP via SecurityWeek and from Nextgov.

SOURCES

Commerce Department moves to close AI chip loophole - Reporting / context

Trump Administration Moves to Block China From Indirect Access to American AI Technology - Reporting / context

U.S. Restricts Overseas Cloud Access to Advanced AI Chips to Close China Export Loophole - 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.