It's Probably Nothing
by Sierra Echo Charlie

EDITION 37 / 27 NOVEMBER 2026

Drupal’s first installer fix wasn’t enough

Mitel flaws go on CISA’s list, and CircuitVerse pulls 40 desktop build artefacts.

5 stories / Listen online - 3:22

THE TAKEAWAY

Drupal has a second fix out for the installer issue we covered earlier this week. The first one left some sites open to takeover, and Drupal says attackers are exploiting that gap. Meanwhile, CircuitVerse had to pull desktop builds from a pipeline that ran malicious code without merging a single affected pull request.

01 / THE BRIEF

Drupal ships a second fix for an exploited installer flaw

The new advisory covers CVE-2026-136716. Drupal says some production sites with unusual or incomplete installations can still be taken over after the first patch if their installer is reachable remotely. Sites that had already secured the installer aren’t vulnerable through this route.

WORTH ASKING

The fixed releases are 10.6.23, 11.3.23 and 11.4.14. On affected production sites, run Drupal’s database update after upgrading, then check site logs for unauthorised access, especially unexpected changes to or activity by the user 1 account.

SOURCES

Drupal core - Highly critical - Access bypass - SA-CORE-2026-019 - Primary source

Drupal 11.4.14 release notes - Primary source

Drupal: rilevato sfruttamento in rete della CVE-2026-136716 - Primary source

Actively Exploited Drupal Installer Access Bypass Can Enable Site Takeover - Reporting / context

02 / THE BRIEF

Five Mitel MiCollab flaws land on CISA's known-exploited list

Accenture investigated one compromise that began before Mitel's 16 November patch. The attacker reached a domain controller within 32 minutes of the first request investigators observed. That's one incident, not a measure of how widely the flaws have been used.

WORTH ASKING

MiCollab build 10.3.0.18 still needs the separate patch or an upgrade to a release that includes the fix. If patching has to wait, Mitel recommends restricting external access to conferencing. For compromise checks, Accenture points to upstream logs and the directory, not just the appliance.

SOURCES

CISA Adds 10 Known Exploited Vulnerabilities to Catalog - Primary source

Mitel Product Security Advisory MISA-2026-0012 - Primary source

When patch day comes too late - Primary source

03 / THE BRIEF

CircuitVerse pulls 40 build artefacts after malware runs in CI

CircuitVerse confirmed that the PolinRider loader ran in its desktop build pipeline in October. None of the affected pull requests was merged, but the maintainers deleted all 40 associated build artefacts. That's a count of files pulled, not downloads or infections.

AsyncAPI's approval requirement stopped the affected fork workflows from running. At CircuitVerse, the merge boundary held; it just wasn't the boundary that controlled who could publish a build.

SOURCES

CircuitVerse issue #1586: malware in pull requests and build CI - Primary source

PolinRider Malware Force-Pushed Into AsyncAPI, CircuitVerse and Open Food Facts Pull Requests - Primary source

PolinRider Plants Python Loaders in 375 GitHub Repositories Using Ethereum - Reporting / context

04 / THE BRIEF

Peninsula confirms shutdown at its Wyoming uranium project

In a 25 November ASX filing, Peninsula Energy confirmed a precautionary shutdown at Lance. It says the incident appears confined to plant and wellfield operating and control systems, with administrative systems in Australia and the US unaffected. Operations won't resume until recovery and safety checks are complete. There's no restart date, and the effect on 2027 production guidance is still unclear.

SOURCES

Peninsula Provides Update on Lance Cyber Security Incident and Recovery Program - Primary source

Wyoming uranium operation shuts down after cyberattack - Reporting / context

05 / THE BRIEF

Todoist confirms stolen tokens were used to read task data

Todoist's roughly 6% figure is for downloaded legacy account records, not task data. Stolen Todoist API and Slack tokens affected about 0.003% of users, and attackers used Todoist tokens to access projects, tasks and comments for a smaller subset. For the roughly 0.001% with affected Outlook connections, recorded requests sought message previews and attachment information, not full message bodies.

WORTH ASKING

If Todoist notified you that affected content held credentials, revoke and replace them.

SOURCES

Security incident in November 2026 - Primary source

Todoist Breach Exposes 6% of Users' Account Data and Integration Tokens - 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.