It's Probably Nothing
by Sierra Echo Charlie

EDITION 09 / 23 OCTOBER 2026

eMudhra plans its TLS exit. One private key was 4.

GitLab and Node.js fixes, ConnectWise attribution, and a New Zealand breach disclosure.

5 stories / Listen online - 3:18

01 / THE BRIEF

eMudhra commits to leaving global TLS

eMudhra's board has decided to withdraw from the global SSL/TLS certificate business. The follow-up to the compromised-intermediates story is quite something.

Aikido's analysis says all eight affected private keys were integers below 256; one was 4. eMudhra's preliminary explanation points to a key-generation wrap/unwrap step producing weak keys that were mistakenly published. It denies an infrastructure compromise and says those intermediates issued no end-entity certificates. The root-cause investigation remains open.

The company promises free replacements through partners and continued revocation/status services until issued certificates expire or are replaced.

SOURCES

eMudhra to Exit global SSL/TLS Certificate Business - Primary source

eMudhra Statement on distrust of select Global TLS Intermediate and one Root CA - Primary source

eMudhra CA compromise: eight private keys, and one of them is 4 - Primary source

eMudhra kills its certificate business after researchers cracked its private keys in under a second - Reporting / context

eMudhra Intermediate Key Compromise Triggers Firefox Blocks and Emergency Go Updates - Reporting / context

02 / THE BRIEF

GitLab fixes unauthenticated RCE across seven branches

GitLab has fixed CVE-2026-110264, an integer overflow when compiling a crafted regular expression that can, under certain conditions, allow unauthenticated server-side code execution. CE/EE releases back to 7.0 are affected; the full exploitation conditions aren't disclosed.

Fixes are in 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10 and 18.11.13. GitLab.com is patched. Self-managed operators have a scheduling wrinkle: the upgrade includes database migrations, and GitLab warns of downtime on single-node installations.

QUALIFICATIONS

The release notice doesn't establish in-the-wild exploitation.

SOURCES

GitLab Critical Patch Release: 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10, 18.11.13 - Primary source

GitLab Patches CVSS 10.0 Unauthenticated RCE Affecting Releases Back to Version 7.0 - Reporting / context

03 / THE BRIEF

Node.js Brotli RCE reaches beyond inbound requests

Node.js has also fixed an RCE, CVE-2026-111497, in Brotli decoding. Exposure depends on your application or a dependency decompressing attacker-controlled data; Node.js doesn't do that automatically.

Vercel says it demonstrated memory disclosure and command execution on unpatched supported versions. Its WAF blocks the inbound path, not malicious responses your service fetches. That distinction is worth checking before calling the edge rule a fix.

Patched versions are 22.23.4, 24.22.1 and 26.12.1. End-of-life Node.js 20 won't receive this fix.

SOURCES

Wednesday, October 21, 2026 Security Releases - Primary source

Node.js security advisory: Brotli decoder RCE (CVE-2026-111497) - Primary source

04 / THE BRIEF

Microsoft attributes ConnectWise compromise to Storm-0940

Microsoft now attributes the ConnectWise multi-tenant application compromise to China-state-aligned Storm-0940. It reports attempted sign-ins against more than 2,250 tenants, not 2,250 confirmed compromises.

Microsoft also says the actor used ARTEX agentic AI to accelerate reconnaissance, password spraying and OAuth abuse. Across the broader ARTEX campaign, it reports multiple cases progressing from initial targeting to privileged cloud access in less than three hours.

The persistence detail deserves attention: Microsoft observed follow-on application credential and privilege changes that can outlast remediation of the original app. It cautions that even successful authentication doesn't establish data access or exfiltration.

SOURCES

AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise - Primary source

Storm-0940 ARTEX attacks: ConnectWise app abuse and Okta sign-ups - Primary source

Compromised ConnectWise Backup Credential Enables Access to 162 Microsoft 365 Tenants - Reporting / context

05 / THE BRIEF

Fisher & Paykel Healthcare discloses personal-information exposure

Closer to home, Fisher & Paykel Healthcare disclosed unauthorised access to two employee email accounts and a subset of company files, some containing personal information. It says it's notifying affected people and has notified authorities.

The company reports no evidence that its patient-data system was compromised, and no impact on products, manufacturing or supply chain. It believes the incident is contained. The affected-person count, access method and intrusion date remain undisclosed.

SOURCES

F&P Healthcare statement regarding cyber incident - Primary source

New Zealand's Fisher & Paykel Healthcare hit by cyber breach - 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.