It's Probably Nothing
by Sierra Echo Charlie

EDITION 06 / 21 OCTOBER 2026

Leaked CA keys, a hijacked backup tool and open AI panels

Go wants a rebuild, AOMEI hasn't told anyone, and AI-agent crims forgot to lock the door.

3 stories / Listen online - 5:14

THE TAKEAWAY

Three stories today, and two of them are about software you trusted doing the thing you trusted it for, just on someone else's behalf. The third is about attackers automating their way into shops and leaving the control room open.

01 / THE BRIEF

Eight eMudhra intermediate CA keys compromised, and Go wants you to rebuild

Mozilla says it got a report at 20:06 UTC on Saturday 17 October that private keys for eight eMudhra intermediate certificates had been compromised. Those keys could be used to issue fraudulent HTTPS certificates for sites the attacker doesn't control. Firefox users mostly never noticed. Mozilla pushed a OneCRL block that had reached standard installs by 22:59 UTC the same day, with no update or restart needed. Since then it has shipped Firefox 158.0.1, ESR 115.43.1 and ESR 153.5.1 for people whose settings might have blocked that, plus NSS 3.131.1, which removes the signing root entirely.

Go is where the real work is. Go 1.27.3 and 1.26.10 block 'a small set of intermediate certificates due to specific security concerns around their operation'. That's CVE-2026-111943, and Go recommends upgrading immediately. Go doesn't name the CA, but a commenter on the Go issue matched all eight hashes to eMudhra intermediates. By that mapping, six are TLS intermediates under emSign Root TLS CA - G3 and two are code-signing intermediates under emSign Root CS CA - G3. The Hacker News hasn't verified that match. If it holds, this stops being purely a TLS story.

Go's verifier doesn't do revocation checks or read browser blocklists, so nothing is protected until you rebuild. The Hacker News reports that the filter matches on public-key hashes, which catches cross-signed copies too, and that it can't be disabled. It also reads the filter as applying to custom trusted roots, though Go hasn't said whether that's intended. Go 1.25 and older get no fix. eMudhra hadn't said anything publicly as of 20 October, and nobody has explained how the keys got out. It's also not established what Chrome, Apple or Microsoft are doing about it.

WORTH ASKING

If you ship Go services, rebuild them. If anything you run chains through emSign G3 intermediates, it'll need a certificate from a different intermediate, or patched Go clients will stop connecting.

QUALIFICATIONS

The root cause is undisclosed, the TLS/code-signing split rests on an unverified community mapping, and other root programmes' responses are unknown.

SOURCES

Protecting Firefox users following the compromise of eMudhra intermediate certificates - Primary source

[security] Go 1.27.3 and Go 1.26.10 are released - Primary source

Go Issues Emergency Update Blocking Eight CA Keys Over Undisclosed Security Concerns - Reporting / context

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

02 / THE BRIEF

AOMEI confirms the update hijack but hasn't told infected customers

Last week Google's threat intel group and ManageEngine described UNC7017 tampering with AOMEI Backupper's update configuration. On 20 October AOMEI confirmed it to Recorded Future News: attackers repeatedly altered config files on its update servers between April and July, redirecting downloads to malware for minutes at a time. AOMEI also said it hasn't yet identified or notified infected customers. It has put out a free detection tool instead.

The technique was neat in an unpleasant way. According to BleepingComputer, the attackers edited down_html.ini and Notifycfg.ini and changed the expected checksum, so the malicious ZIP passed verification and ran without any user interaction. From there, the CROSSROAD downloader set up a scheduled task, and the SHINYROAD backdoor used legitimate Radmin components to reach its C2. In the 20 July window, an invisible pop-up also tried to coerce NTLM hashes to an attacker-controlled WebDAV server. The Record says that could work even where the malware itself was blocked.

The identified windows are 28 May 05:40-05:50 UTC, 16 July 08:33-08:39 UTC and 20 July 10:35-10:40 UTC. Google thinks there was probably more tampering it couldn't see. Victims span almost a dozen countries, Australia among them. ManageEngine says it warned AOMEI in June, that AOMEI initially blamed in-transit interception, and that the attackers struck at least twice more after that. ManageEngine also says AnyViewer was targeted, while AOMEI says only Backupper showed anomalies. Attribution is open: the malware avoids machines that appear to be in China, but researchers say that doesn't tell you where the attackers are.

WORTH ASKING

If Backupper was on your fleet between April and July, hunt across that whole period. The server fix doesn't clean machines that were already infected.

QUALIFICATIONS

The primary GTIG and ManageEngine reports weren't read, and ManageEngine hasn't verified that the attackers have lost access.

SOURCES

AOMEI yet to notify customers after hackers hijacked its software updates - Reporting / context

Hackers hijack AOMEI update servers to secretly spread malware - Reporting / context

Ephemeral AOMEI Update Tampering Redirects Downloads to Malware - Reporting / context

03 / THE BRIEF

AI agents hacking shops, watched through their own unlocked panels

NorForge found more than 20 exposed panels for Cairn, an AI agent harness, that it assesses as likely malicious. Through them it could watch agents choose targets and go to work. The biggest cluster, AIA0001, operates in Chinese and runs over 1,100 projects across 14 panels, mostly against the US, Japan and Australia. Its task feed picks e-commerce sites with 200,000-1.5 million in traffic that Playwright has confirmed can actually take orders. The agents are told to find unauthenticated RCE and plant an uploader shell. The worker is named 'claudecode_deepseek-v4.1-flash', which NorForge says 'could mean' Claude Code driving DeepSeek. Its own rough estimate is about a 10% success rate at around US$5 a task, with considerable uncertainty. One of its case studies is an Australian shop with command execution on the web server.

Citing Reuters, Tom's Hardware reports that the agents tried more than 1,200 sites and got into more than 100, including Deere and SharkNinja. SharkNinja says only a product-support information site was affected.

Then there's the self-own. Trufflehog over the panel data turned up hundreds of secrets, 11% of them verified valid, and the panels appeared to expose full admin controls without authentication. NorForge says it didn't test those controls. Cheap, patient, automated exploitation is the worrying bit. The attackers forgetting a login page is just the funny bit. NorForge says it's working with Reuters to notify victims and chase takedowns.

QUALIFICATIONS

The Reuters original wasn't read, and timing may straddle the start of this coverage window.

SOURCES

Inside Cairn: Open Windows into massive AI-Driven Cyber Operations - Primary source

A Chinese hacker used AI agents to break into more than 100 company websites - Reporting / context

AI Platform Cairn Abused to Hack Over 100 Organizations - Reporting / context

Exposed AI Agent Panels Reveal Reported Breaches of More Than 100 Websites - 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.