ISSUE #006 · FALSE ASSURANCE

False Assurance.

A git tag rewritten in fifteen minutes. An AWS account that walks away from every SCP (Service Control Policy) and detection your central console assumes is watching it. Azure VMAccess detection guidance blind to the attacker's chosen extension name. An AI framework whose session refresh can be abused cross-origin.

> ATTACK

Ilyas Makari at Aikido · 2026-05-23 · **Supply Chain Attack Targets Laravel-Lang Packages with Credential Stealer**

An attacker with push access to the Laravel-Lang GitHub org used a feature most defenders forget: GitHub lets a tag in one repo point at a commit in a fork of that repo. ~233 versions across `laravel-lang/lang`, `/attributes`, `/http-statuses` re-pointed at commits in a malicious fork. Composer pulled the tag (Composer is PHP's package manager; its autoloader runs files listed in `autoload.files` at app boot), the autoloader pulled `src/helpers.php`, and two innocent helpers (`laravel_lang_locale`, `laravel_lang_fallback`) sat above a self-executing block that fingerprints the host, fetches `flipboxstudio[.]info/payload`, runs the returned PHP, and exfiltrates to `/exfil`.

Payload is a 5,900-line PHP stealer covering nine cloud providers, kubeconfig, Vault tokens, Docker configs, Helm repos, SSH keys, git credentials, package-manager auth, shell history, plus stored secrets from browsers, cryptocurrency wallets, and chat platforms. **A git tag is a mutable pointer to a commit. Any toolchain that pulls a package from Git by tag is one push away from this class of attack.**

▸ SHIP THIS WEEK

Audit `autoload.files` entries everywhere Composer wires them in: your project's `composer.json`, every dependency's `composer.json`, and the generated `vendor/composer/autoload_files.php` that aggregates them. Composer runs every file in that list as soon as PHP loads the autoloader, on every app boot. For any VCS-sourced dependency, pin to an immutable commit reference rather than a tag. Grep CI logs, dev workstation shell history, and outbound DNS for `flipboxstudio.info`, `laravel_lang_locale`, `laravel_lang_fallback`.

> RULE

Shannon Brazil, Richard Billington, and Derek Ramirez at AWS CIRT · 2026-05-19 · **CIRT insights: How to help prevent unauthorized account removals from AWS Organizations**

Alert on CloudTrail events `LeaveOrganization` (the API a member account uses to detach itself from the AWS Organization), `RemoveAccountFromOrganization`, `AcceptHandshake`, `InviteAccountToOrganization`. The moment a compromised member account leaves: it exits SCP enforcement, CloudTrail org trails stop capturing it, GuardDuty findings stop flowing. The central console keeps looking normal. Deploy `DenyLeaveOrganizationSCP` at the org root. Ship the detection and the SCP together. One catches the escape attempt, the other refuses it.

> DEFENDER

Lydia Graslie at Sysdig Threat Research · 2026-05-20 · **The expendable extension name: Azure VMAccess naming chaos, password resets, and a detection gap**

Two distinct gaps in Sysdig's reproduction of Microsoft's Azure Threat Research Matrix VMAccess guidance. First, name-based rules on `Microsoft.Compute/virtualMachines/extensions/write` miss the attack when the attacker picks an arbitrary extension name (the resource name is a caller-controlled string). Second, Sysdig's reproduction produced zero `validate/action` events for `vmaccesswindowspasswordreset`, the canonical ATRM signal, regardless of naming. Microsoft on naming: documented behavior, resource names are user-specified. Sysdig's alternative: alert on `extensions/write` broadly, correlate via Azure Resource Graph (Azure's inventory query layer for resource metadata) against `Microsoft.Compute/virtualMachines/extensions` to recover the real publisher and type.

> RADAR

Merav Bar and Rami McCarthy at Wiz · 2026-05-13 · **Fragnesia: Linux Kernel Local Privilege Escalation via ESP-in-TCP**

A patch addressing the original Dirty Frag vulnerabilities introduced a deterministic page-cache corruption primitive: controlled single-byte writes into cached file pages via AES-GCM keystream manipulation. Public PoC. The regression surface for any kernel patch extends well past the single bug it was named for.

CISA · 2026-05-21 · **Langflow CVE-2025-34291 added to Known Exploited Vulnerabilities catalog**

NVD CVSS v3.1 8.8 High; VulnCheck CNA CVSS v4 9.4. Affects Langflow through 1.6.9. Second KEV entry following CVE-2025-3248. Treat code-execution endpoints on internal AI tooling the way you treat `kubectl exec` on production clusters.

SOURCES

Aikido / aikido.dev/blog/supply-chain-attack-targets-laravel-lang-packages-with-credential-stealer
AWS CIRT / aws.amazon.com/blogs/security/cirt-insights-how-to-help-prevent-unauthorized-account-removals-from-aws-organizations
Sysdig / sysdig.com/blog/the-expendable-extension-name-azure-vmaccess-naming-chaos-password-resets-and-a-detection-gap
Wiz / wiz.io/blog/fragnesia-linux-kernel-local-privilege-escalation-via-esp-in-tcp
CISA / cisa.gov/known-exploited-vulnerabilities-catalog
Chris Farris / chrisfarris.com/post/security-poverty-cliff