THE FORENSICS WAY

ISSUE 39 | FORENSICS AWARENESS THIS WEEK | TUESDAY, OCTOBER 27, 2026

FRONT PAGE

WEB INFRASTRUCTURE

PHP2Shell: Two Pre-Auth Flaws in the Runtime Underneath Most of the Web, Disclosed by an Embargo That Broke Early

CVE-2026-109618, a memory corruption bug, and CVE-2026-109619, a stale internal request-state bug, each give unauthenticated remote code execution at CVSS v4 9.2. CISA's assessment is that they affect every PHP installation serving web requests — mod_php, PHP-FPM, php-cgi, FrankenPHP and LiteSpeed — with mod_php carrying the highest risk. The embargo broke on October 20, ahead of the planned coordinated release; PHP shipped 8.5.12, 8.4.27, 8.3.36 and 8.2.35 the following day, CISA issued an alert the same day, and both CVEs reached the KEV catalogue on October 26 with an October 29 remediation date. Unsupported branches, PHP 5 among them, are reported affected with no fix coming.

Exploitation reporting is genuinely mixed: honeypot operators report attempts in the wild, while Rapid7 says the public proof-of-concept code works only against particular combinations of operating system, PHP version and web server. Unpatched is therefore not the same as compromised, and saying so is part of the job. Forensic priority: execution lands as the web worker and need not drop a file, so the web server access and error logs are the primary record — preserve them before rotation, and scope the hunt to the window between the embargo break and your patch. PHP-FPM recycles its workers, which destroys process state, so if a host is still suspect, capture memory before anything restarts the service.

TRUST INFRASTRUCTURE

Eight Keys Anyone Could Have Computed: A Flawed Key Ceremony Put Weak eMudhra Intermediates Into Every Trust Store

Private keys for eight eMudhra intermediate CA certificates are compromised — not stolen, but weak enough to derive. eMudhra attributes this to a flaw in its April 2025 key ceremony that produced a second, weak set of keys, and it was that set which went

THREAT BULLETIN

Critical

CVE-2026-111497 — Brotli, as bundled by Node.js and others. An out-of-bounds write in Google's Brotli decoder affecting versions 1.0.3 through 1.2.0: a crafted stream can crash a process, leak memory or lead to code execution. CVSS v4 9.2, though Node.js rates it High. Disclosed October 21 and fixed in Node 22.23.4, 24.22.1 and 26.12.1, with Node 20 and earlier unfixed and Bun needing 1.4.4. Named Node2Shell, then widened to HTTP2Shell once Python Brotli packages and other HTTP stacks proved affected. *Forensic Note:* Exposure is a dependency question, not a product one — enumerate everything that decompresses attacker-supplied Brotli, including Express 5's default JSON body handling.

Active Exploit

CVE-2026-110447 — Collabora Online built-in CODE Server, as used within Nextcloud. An OS command injection yielding remote code execution, with the notable precondition that it applies when the CODE server is not running. CISA KEV October 23, due October 26. *Forensic Note:* Because the flaw depends on a stopped service, pull service start and stop history and reconcile it

to the browser root programmes; published analysis describes each P-384 private value as below 256, recoverable from the public certificate in under a second. A researcher reported it to the root programmes on the evening of October 17 and it became public on October 20. Chrome and Firefox blocked the intermediates from October 17, Apple from October 19 and Microsoft from October 20.

Chrome reported that no TLS certificates chaining to the six website-facing intermediates had been logged to Certificate Transparency before the block, and eMudhra says it has no evidence the weak keys were recovered or abused before disclosure. What remains exposed is everything that is not a browser: API clients, containers, build pipelines and embedded devices that carry their own CA bundles and never check revocation or CT. Cloudflare now rejects these certificates in its Workers and Pages build images and has flagged that custom *SSL_CERT_FILE* or *REQUESTS_CA_BUNDLE* settings need updating by hand. Forensic priority: CT logs are the evidentiary record, and for the web-facing intermediates the absence of a logged certificate is a real negative finding. Everywhere else, the question is an inventory one — find out where your trust stores actually live before you assume a browser vendor fixed this for you.

against request logs — an outage window is the thing to hunt around, not an anomaly to dismiss.

Malware Spotlight

ARTEX — The Intrusion Handed Over to an Agent

Microsoft Threat Intelligence reported on October 21 that China state-aligned Storm-0940 used ARTEX, an open-source agentic AI penetration-testing framework, to automate attacks against hundreds of organisations from around September 2026, and assesses the actor responsible for the ConnectWise supply chain compromise of a multi-tenant application. In several cases under three hours elapsed between initial targeting and privileged access to cloud infrastructure. The actor authenticated into Microsoft 365 through already-authorised compromised applications, avoiding interactive user sign-in altogether. *Forensic Note:* No user sign-in means no sign-in log to alert on, so pivot to service principal and OAuth application activity — and read the compression of the timeline itself as evidence, because a human-paced playbook does not reach privileged access in under three hours.

THE FORENSICS WAY

HISTORICAL ARCHIVES HISTORY OF DIGITAL INVESTIGATION TUESDAY, OCTOBER 27, 2026

CASE STUDIES: HISTORICAL GRID

SHELLSHOCK (2014)

Twenty-Five Years in the Shell: The Pre-Auth Flaw That Made Web Logs the Only Witness

Disclosed on September 24, 2014, CVE-2014-6271 let bash execute commands appended to an environment variable's function definition, and anything that passed attacker-controlled data into the environment of a shell — above all CGI, where headers become environment variables — became a pre-authentication remote execution path. The bug had been present for roughly twenty-five years. Mass scanning began within hours, the initial patch proved incomplete and five further CVEs followed within a week, so defenders patched against a moving target while exploitation was already underway. Forensically it set the pattern this week's PHP flaws repeat: execution happened inside the web server's own process, dropped nothing by default, and left a record only in request logs — which is why the first instruction in 2014, as now, was to preserve those logs before they rotated.

DIGINOTAR (2011)

Five Hundred Fraudulent Certificates: The Investigation That Ended a Certificate Authority

In mid-2011 an intruder reached the certificate infrastructure of the Dutch CA DigiNotar and issued at least 531 fraudulent certificates, including one for **.google.com* later used to intercept the traffic of an estimated several hundred thousand Iranian users. The investigation, published as Operation Black Tulip, found the CA's systems poorly segmented, its logging incomplete and its issuance records unreliable — so investigators could not state with confidence how many certificates had been issued, only a floor. Browsers removed DigiNotar from their trust stores within days and the company was bankrupt within weeks. It remains the reference case for why Certificate Transparency exists, and the reason this week's eMudhra story turns on what was logged rather than on what the CA says happened.

VPNFILTER (2018)

The Reboot That Destroyed the Evidence: Half a Million Routers and a Stage That Only Existed in Memory

In May 2018 Cisco Talos disclosed VPNFilter, modular malware on at least 500,000 consumer and small-office routers and NAS devices across 54 countries, and the FBI seized its fallback domain to sinkhole the botnet. Stage one persisted across reboot purely to re-establish contact, while stages two and three — credential collection, packet sniffing and a destructive firmware-overwrite command — lived only in memory and vanished when a device was power-cycled. The FBI's public advice to reboot mitigated the threat and erased the evidence in one action.

CODE RED (2001)

A Worm That Never Touched the Disk: The First Mass Incident Investigated From Memory and Traffic Alone

From July 2001 Code Red spread through a buffer overflow in Microsoft IIS, infecting on the order of 359,000 hosts in under fourteen hours at its peak. It wrote no file to disk, existing only inside the *inetinfo.exe* process, so a reboot removed it entirely and left an administrator with no artefact to examine. Investigators reconstructed the outbreak from network telemetry, defaced response pages and live process state rather than imaged media.

TOOLS OF THE TRADE

OPEN SOURCE

ALEX

V0.7 — ANDROID

Android Logical Extractor, which in this release adds Dirty COW and CVE-2016-10277 exploit support for older devices, offline ADB backup decryption and better SU manager detection. The value is reach into handsets too old for current commercial support but still turning up in casework.

COMMERCIAL

CapLoader

2.2 — NETRESEC

Flow-level PCAP triage that now alerts on commonly abused services — IPFS gateways, VPN and proxy protocols, blockchain RPC nodes and paste sites — and accepts external blocklists. Also fixes JA4 fingerprinting for GREASE values, which matters if you fingerprint clients from capture.

UTILITY / SCRIPT

ORISA

GEORGIA TECH — IEEE S&P 2026

Recovers deleted on-device AI assistant conversations from Android memory and rehosts the fragments as a working session. Across 60 configurations spanning ten apps and three models it recovered chat content; in one test the restored session surfaced 26 planted facts against the original's 14.

UTILITY / SCRIPT

Obliterator 3

METASPIKE — FREE

Command-line batch remediation across mailboxes via EWS, IMAP and Graph, extended in v3 to Google Drive, OneDrive and SharePoint. Keeps a resumable project database and writes protocol logs with built-in verification — so a deletion campaign produces its own defensible record.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-21589 (ATLASSIAN DATA CENTER)

Unauthenticated file read from the web root (CWE-552) across eight self-hosted products, exploited within hours of a public technical write-up; CVSS 9.3, CISA KEV October 15. *Forensic Note:* A file read raises no application audit event, so web and proxy logs from every cluster node are the record.

ARCHIVE ALERT

CVE-2026-102764 (BEYONDTRUST REMOTE SUPPORT)

Improper origin validation (CWE-290) in an internal messaging component allowing file operations on the appliance; CVSS 9.3, KEV October 16, exploitation traced to August 29. *Forensic Note:* Dwell time predates disclosure by seven weeks — longer than many appliances retain logs.

RECENT MALWARE WATCH

ARCHIVE: OCTOBER 20, 2026

PEERSTITCH — THE IMPLANT WITH NO FILE, PORT OR CALLBACK

Unit 42's memory-resident ARM64 FortiGate implant, running inside the miglogd and iked daemons via ptrace with no persistent binary on disk, used to exfiltrate 500+ firewall configurations. Capture process memory before any reboot.

ARCHIVE: OCTOBER 13, 2026

MATCHBOIL / MATCHWOK — FROM MINISTRIES TO THE POWER GRID

Russia-aligned UAC-0099's C# downloader and its MATCHWOK backdoor payload, delivered through phishing impersonating Ukrainian court summonses, with targeting shifted to transport, manufacturing and energy.