THE FORENSICS WAY

ISSUE 38 | FORENSICS AWARENESS THIS WEEK | TUESDAY, OCTOBER 20, 2026

FRONT PAGE

EDGE DEVICE INTRUSION

Clean Integrity Check, Compromised Appliance: Chained Ivanti Zero-Days Left Almost Nothing on Disk to Find

Volexity published its analysis on October 13 of a chain against Ivanti Connect Secure that produces unauthenticated root-level command execution. CVE-2026-104935 covers an authentication bypass — a request to the public *welcome.cgi* naming a protected script in the *X-DSCGI-PATH* header reaches it without credentials — together with a race-condition file write in *wu.cgi*, where an upload lands on disk before validation and is executed in the window before deletion. A third flaw, privilege escalation through the *dsinvoked* broker trusting DSCache configuration data, has no CVE and no fix yet. Exploitation began October 3 against a fully patched appliance; Ivanti patched on October 13, the day CISA added the CVE to KEV. Volexity attributes the activity to a previously unknown actor, UTA0576.

No web shell, backdoor or first-stage binary was deployed: commands and their output travelled inside the exploit's own HTTPS requests. The payload truncates */home/runtime/dlogs/debuglog* and */var/log/audit/audit.log* across the targeted window, deletes its own scripts, restores the modified DSCache entry and keeps the library patch in memory only, so Ivanti's Integrity Checker Tool reports no modification at all. Forensic priority: treat a clean integrity check as no evidence. Memory acquisition from the live appliance recovered the operator tooling, output and packet captures; look for */data/.icscap/* holding *cap** files and a renamed tcpdump running as *dsstatmond*, and web logs where the request path and the *X-DSCGI-PATH* header disagree. Post-exploitation took LDAP credentials, LAPS passwords and BitLocker recovery keys, so scope the domain, not the box.

FORENSIC CAPABILITY

Keeping Pace With the Evidence: Europol and the Commission Publish a Gap Analysis of EU Digital Forensics

On October 16 the European Commission, working with Europol, published *Digital Forensics: Gap Analysis*, an assessment of digital

THREAT BULLETIN

Active Exploit

CVE-2026-21589 — Atlassian Data Center. Files accessible to external parties (CWE-552) lets an unauthenticated attacker read files from the web root, though only at a known exact path. CVSS 9.3, across eight self-hosted products including Confluence, Jira, Bitbucket and Crowd; Cloud tenants are unaffected. Honeypots saw exploitation within hours of watchTowr's write-up, and in Crowd SSO deployments the read can be leveraged into administrator takeover. CISA KEV October 15. *Forensic Note:* A file read raises no application audit event, so the web and proxy access logs are the only record — and they must be pulled from every cluster node, Bitbucket mirrors included.

Critical

CVE-2026-102764 — BeyondTrust Remote Support. Improper origin validation (CWE-290) in an internal messaging component allows a remote attacker to perform file operations on the appliance; CVSS 9.3, advisory BT26-05 of October 15, KEV October 16. CISA reports actors using it for initial access and then persisting, escalating and moving laterally, and Mandiant ties the activity to a suspected

forensic capability across the member states mandated under the June 2025 Road Map on lawful access to data. Its central finding is that authorities are short of both resources and skills and are struggling to keep pace with new technologies, that capability varies widely between member states, and that commercial tooling is expensive and ages quickly. The priority areas it names are standardisation and interoperability of tooling, cloud, IoT and vehicle forensics, AI within legal limits, and training gaps reaching beyond examiners to first responders and legal professionals.

The report asks for sustained investment and closer cooperation between law enforcement, researchers, tool developers and manufacturers — and it lands in a week that demonstrates the gap in practice. An intrusion that leaves no file on disk, no listening port and a truncated audit log is provable only by someone equipped and trained to acquire volatile memory from a vendor appliance before it is rebuilt. Forensic priority: read the gap analysis as a procurement and training argument you can cite. The capability it calls unevenly distributed — memory forensics, appliance acquisition, tool validation — is exactly what this week's two intrusion stories demand, and its absence is the difference between a finding and an assumption.

PRC-nexus group with compromises dating to August 29. *Forensic Note:* Disclosure trails first exploitation by about seven weeks, longer than many appliances retain logs — collect appliance logs and session recordings before patching, then rotate every credential it could reach.

Malware Spotlight

PEERSTITCH — The Firewall Implant With No File, No Port and No Callback

Unit 42 research this week details a memory-resident ARM64 implant on FortiGate firewalls, used by the cluster it tracks as CL-STA-0954 against a telecom managed service provider, from which more than 500 firewall configurations were exfiltrated. The actor reached FortiManager first through FortiJump (CVE-2024-47575), then deployed the implant using CVE-2025-61624, a FortiOS auto-script path traversal fixed in April 2026 and added to KEV on October 16. PEERSTITCH leaves no persistent binary, opens no listening port and makes no outbound connection, running instead inside the *miglogd* and *iked* daemons by manipulating their memory via ptrace. *Forensic Note:* A disk image of the appliance will show nothing, so capture process memory before any reboot, and hunt auto-script object names containing ../ sequences.

CASE STUDIES: HISTORICAL GRID

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 *toknowall.com* fallback domain to sinkhole the botnet. Its architecture made it a forensic problem in its own right: stage one persisted across reboot purely to re-establish contact, while stages two and three — credential collection, packet sniffing, Modbus inspection and a destructive firmware-overwrite command — lived only in memory and vanished the moment a device was power-cycled. The FBI's public advice to reboot therefore mitigated the threat and erased the evidence in one action. It remains the clearest demonstration that on network appliances the disk is not where the case is, and that a remediation step can be anti-forensic by accident.

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, which meant a reboot of an affected server removed it entirely and left an administrator with no artefact to examine. Investigators at CAIDA and elsewhere reconstructed the outbreak from network telemetry, defaced response pages and live process state rather than imaged media, and the resulting propagation model became a reference for later worm analysis. Code Red set the precedent that whole classes of compromise are observable only while still running — the constraint that governs this week's appliance implants, twenty-five years on.

THE GERMAN STEEL MILL (2014)

A Furnace That Could Not Be Shut Down: The Case That Proved Code Could Break Metal

Germany's federal information security agency, the BSI, disclosed in its December 2014 annual report that attackers had phished their way into a steel mill's office network, pivoted into the production network, and left a blast furnace unable to be shut down in a controlled manner — causing what the agency called massive physical damage. The report credited the attackers with detailed knowledge of industrial control systems, named neither the plant nor an actor, and published almost no technical indicators. That silence became its own lesson: it

MAROOCHY SHIRE (2000)

Forty-Six Radio Commands: The First OT Intrusion Investigated Well Enough to Convict

Across February to April 2000, Vitek Boden used a laptop and a two-way radio to issue commands to sewage pumping stations in Maroochy Shire, Queensland, releasing on the order of 800,000 litres of raw sewage into parks, waterways and hotel grounds. He had worked for the contractor that installed the SCADA system, so his instructions were indistinguishable from legitimate ones in isolation. Investigators built the case by correlating radio telemetry against pump-station alarms to separate attack from malfunction, then recovered the control

remains one of the most-cited OT incidents precisely because so little evidence was ever released.

software and command traces from the seized laptop. It stands as the earliest OT compromise investigated thoroughly enough to secure a conviction.

TOOLS OF THE TRADE

OPEN SOURCE

Regipy

V6.5.0 — PLUS RUST PORT

Python library and command-line tool for offline Windows registry analysis, with plugins that parse hives into structured output rather than requiring a GUI walk. A Rust port, regipy-rs, has begun alpha releases alongside it, aimed at throughput when hundreds of hives arrive at once.

OPEN SOURCE

WEBCQUISITION

AUTOMATED WEB CAPTURE

Drives a Windows VM on VMware Workstation Pro to capture web activity forensically: PCAPNG traffic capture, TLS secrets logged via SSLKEYLOGFILE so HTTPS can be decrypted later, and hashed screenshots. Output is a JSON acquisition record, an HTML report and a hash-chained event log, copied to the host under double SHA-256 verification.

COMMERCIAL

Atola TaskForce

2026.10 — COMPARE MODULE

Imager firmware whose new Compare module checks every sector of a source drive against its image, drive or file, and reports exactly which sectors differ or are unreadable. It also compares sectors against a hex or LBA pattern, answering whether a wipe left the expected byte everywhere when a hash alone cannot.

UTILITY / SCRIPT

UFADE

V1.0.5 — APPLE DEVICES

Universal Forensic Apple Device Extractor, a pymobiledevice3 wrapper that collects a logical backup, crash reports, a sysdiagnose and the Apple Unified Log from an iOS device without a jailbreak. The unified log collection is the useful part, carrying unlock, pairing and process events no backup will give you.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-104286 (FORTINET FORTIMAIL)

Path traversal (CWE-22) with improper NULL-byte handling (CWE-158) gives an unauthenticated attacker arbitrary file write, reportedly via the webmail IBE component; CVSS 9.8, disclosed as an exploited zero-day in FG-IR-26-175. *Forensic Note:* Hunt for files written outside expected directories.

ARCHIVE ALERT

CVE-2026-89111 / CVE-2026-89107 (SAP)

Unauthenticated SSRF in SAP Cloud SDK for Python (CVSS 10.0) redirecting OAuth2 token requests to capture client credentials, alongside ABAP code injection in S/4HANA (CVSS 9.9). *Forensic Note:* Audit OAuth2 token endpoints for requests resolved to unexpected hosts.

RECENT MALWARE WATCH

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. Anchor hunting on the archive-plus-script delivery pattern.

ARCHIVE: OCTOBER 6, 2026

SC — THE WORDPRESS BACKDOOR THAT REBUILDS ITSELF

Sucuri's "self-healing mesh" living in at least eight places at once across files, a database options row and a System V shared-memory segment, where any survivor restores the rest on the next page load. Enumerate all persistence classes before removing any.