DECEPTION CHECK

READER GUIDE / THE PRACTICAL QUESTION

Some VMware admin actions could go unlogged.

What is your second source of evidence?

The issue in plain language

A hypervisor runs virtual machines. Its audit trail records activity on that host. CVE-2026-41709 lets an administrator perform certain ESX operations without those operations being logged. It is a gap after administrator access, not an initial break-in method.

Why it belongs in the response queue

CISA added the issue to its Known Exploited Vulnerabilities catalog on October 28. CrowdStrike reports WARP PANDA exploited the ESXi command-logging bypass in intrusions involving vCenter environments.

Give three people three checks

Platform owner: verify the supported update is running.
Security owner: review administrator access and management exposure.
Response owner: test receipt, retention, and alert ownership for separately collected evidence.

A copy and a second source answer different questions

Forwarding a host log can preserve it. It cannot restore an event the host never emitted. Identity activity, management tasks, and network evidence can answer other parts of the investigation.

This edition includes standard Linux Sigma rules and native platform hunts. The collection-health workflow is a separate engineering design. The article links exact files, setup notes, and the validation record; test the selected route against your own telemetry before enabling alerts.

Broadcom advisory, section 3e

CrowdStrike report

PRODUCT SCOPE / SUPPORTED FIXES

Match the fix to the platform.

ESX 8.0

ESXi80U3j-25429389

ESX 9.0 / VCF or VVF

ESXi-9.0.2.0100-25595025

ESX 9.1 / VCF or VVF

ESXi-9.1.0.0-25370933

Cloud Foundation 5.x

5.2.4; use the vendor component and async-patching guidance.

Telco Cloud Platform 5.0.x / 5.1.x

Follow Broadcom KB 449886, CVE-2026-41709 row and compatibility path.

These are the section 3e response-matrix entries, not fixes for every CVE in the combined advisory. Use current vendor guidance for later releases and unlisted support branches. No workaround is listed.

Federal dates are context, not a universal deadline

CISA lists November 11 for ESX and October 31 for Fragnesia. Covered federal agencies must meet their obligations; other organizations should prioritize by exposure and operational dependency.

Broadcom response matrix

Official CISA KEV data

SEPARATE CASE / PHP2SHELL AND FRAGNESIA

Read the technical chain.

1 / PHP request handling

Dream describes multipart setup, memory exhaustion, pointer disclosure, and stale session state in appweb. Original PHP2Shell: CVE-2026-109618 and CVE-2026-109619.

2 / Web-service execution

The recovered chain executes as nobody in the httpd_t SELinux context before escalating.

3 / Cached policy to root

Fragnesia changes page-cache-backed /etc/pam.d/su rules to use pam_permit.so. The chain then invokes su to become root. Ordinary file-write telemetry can miss this change.

4 / Persistence and tunnel

Reported paths include /unauth/php/change_password.php and /usr/local/lib/.panops/. Scripts use systemd or rc.local; reverse SSH or SOCKS supports further access.

5 / Connected identity

Investigators report LDAP credential extraction and directory enumeration after access to an internal management server. Review the service account and connected identity systems.

Use the vendor boundary

The PAN-OS advisory scopes management HTTPS web UI and XML API access. It says GlobalProtect portal, gateway, and Clientless VPN services are not impacted. Remove public management exposure and use the supported appliance update path.

This is separate from the ESX case. The setup spans multiple requests; artifact paths are leads to compare with a trusted baseline. Fragnesia was disclosed in May. Use the vendor-supported appliance update and forensic path.

PAN-OS advisory and fixed release trains

Unit 42 update

Dream research

FIRST-PARTY EVIDENCE / DIFFERENT LAYERS

One instruction. Two records.

In retained October 1 SSH-decoy records, we compared a key-placement instruction with a matching virtual-file capture from the same session. The submitted key-line hash matched the capture record.

`01:03:28.433307 UTC`

Submitted instruction to place an SSH key in the authorized-keys file.

`01:03:28.613805 UTC`

Matching virtual-file capture recorded in the same decoy session.

What each layer answers

Command input: what was submitted.
Captured artifact: what was retained.
Authentication evidence: whether a key was accepted later.

These are research-decoy inputs and a matching virtual-file capture. They do not establish a production write, later accepted key use, or a link to ESX or Fragnesia.

Where a decoy helps

A decoy adds a signal when someone interacts with it and its collection path is working. Keep legitimate use understood, collection separately controlled, and the alert route tested. It complements platform updates and ordinary monitoring.

SSH key research and method

Response article and static evidence diagram

Start with the logs you have.

Linux process events

Use the standard Sigma rules with product linux and category process_creation. The rules use conventional field names, such as Image, ParentImage, CommandLine, and User. Choose the backend pipeline for your existing telemetry.

Native platform queries

Choose the documented query surface for your product. Check its source requirements and fields, select the appropriate source or device group, and compare returned events with the originals. Product support differs by source; the coverage guide states the available routes.

ESXi shell logs

Use the dedicated native imported-shell hunts. ESXi is not an ordinary Linux EDR endpoint. These searches inspect recorded command activity; they cannot recover an operation that the host never logged.

Collection health

D3 is a stateful monitor design. It needs an expected-asset inventory, independently observed checks, and an owner. It is not shipped as an ordinary Sigma rule or a fictional built-in vendor table.

Before enabling alerts

Start read-only, review false positives, retain source event identity, assign an owner, and test delivery. The validation file names the parser, conversion, and fixture checks actually performed; it does not claim tenant execution.

Full customer detection library

Know what the check can see.

D1 / ESXi syslog configuration command observed

Data: Imported ESXi shell events

Check: A direct captured command starts with esxcli system syslog config set; inspect the configuration result and authorization.

Review: Approved collector migration, certificate or retention tuning, recovery.

Limit: API configuration changes, compound shell commands, encoded commands, omitted shell records, aliases, and alternate tools. A matched command may fail. A set command alone does not prove logging was disabled.

Next action: Preserve remote logs; compare current log destinations and retention to signed baseline through management inventory, inspect the change ticket and account, and check D3. Do not run the matched command.

D2 / Explicit log-file deletion or truncation command

Data: Linux process events; imported ESXi companion for D2

Check: Linux event hunts require a real rm/truncate/shred process Image plus a direct-start command naming an explicit log path. The ESXi companion instead parses a logged shell command; it has no Linux process Image event.

Review: Log rotation, space recovery, support collection cleanup. Prefer narrow approved executable/hash, path, account, and ticket exceptions with expiry.

Limit: Shell redirection, unlink/truncate syscalls inside another process, wildcards relative to working directory, path variables, quoted tool names, encoded commands, API actions, or records never emitted. Successful page-cache writes need not produce a file-write event.

Next action: Preserve existing remote copies and volatile evidence; inspect command result, filesystem state, audit coverage, retention jobs, and recent admin sessions. Avoid restarting or overwriting evidence before triage.

Exact rules, source requirements, and validation

Know what the check can see.

D3 / Detect expected-log loss with an independent monitor

Data: Engineering design only

Check: Engineering workflow over authoritative inventory and independent health evidence; not an ordinary Sigma absence rule.

Review: Network outage, collector routing or parser changes, stale inventory, maintenance, overloaded ingestion, clock errors.

Limit: Design only; no stock table, ordinary Sigma rule, native query, or deployed monitor is supplied. Missing records require authoritative expected inventory. Healthy markers cannot prove every operation was logged.

Next action: Check pipeline delay and queue/drop metrics, maintenance, remote collector receipts, current forwarding config, and independent vCenter/identity/network records. Escalate unexplained loss; preserve existing evidence. A second deadman check must alert if the monitor itself stops publishing.

D4 / Linux web worker launches a shell or executable from temporary storage

Data: Linux direct-parent process behavior

Check: Direct parent basename is apache2, httpd, nginx, php-fpm with optional numeric version, or php-cgi; child basename is a shell or child image path begins /tmp/, /var/tmp/, or /dev/shm/. Count one distinct process start; 15-minute review window.

Review: CGI scripts, application shell helpers, image conversion or job runners. Baseline exact approved path, hash, service and application, rather than allowing all shell children.

Limit: In-process PHP code, webshells that do not spawn a process, renamed web workers, deeper ancestry, dropped telemetry, containers with partial host coverage. This is not a PHP2Shell signature.

Next action: Inspect full ancestry, service identity, requested URL and application logs, executable provenance, outbound connections, and persistence. Isolate through approved incident procedures if corroborated.

Exact rules, source requirements, and validation

Know what the check can see.

D5 / Root-account process below a web worker

Data: Linux direct-parent process behavior

Check: Direct web-worker child is recorded as root; parent identity and a privilege transition are not established.

Review: Approved sudo/setuid application helper or privileged application architecture. Root master spawning a non-root worker is the opposite direction and must not match.

Limit: Root account does not prove non-root parent, privilege transition, kernel exploitation, or host root inside a user namespace. Legitimate root web-service masters may match.

Next action: Verify host versus container/user-namespace identity, legitimacy of privilege helpers, kernel inventory and booted vendor patch, process memory/ancestry, and application evidence. Treat PID reuse as a correlation defect.

D6 / SSH remote forwarding requested below a web worker

Data: Linux direct-parent process behavior

Check: Direct web-worker child requests SSH remote forwarding; no deeper ancestry or established-tunnel claim.

Review: Explicit application support tunnel or remote maintenance integration. Require a documented destination, account, owner, and expiry for exceptions.

Limit: SSH configuration-file RemoteForward, command obfuscation, renamed SSH, other tunnel software, deeper ancestry, shell-string options outside captured argv. -r is different and must not match. The lexical pattern can match option-like text in a remote command; verify SSH argument position. Spelling/case variants may be missed.

Next action: Inspect process ancestry and destination/session evidence, validate the business owner, contain unapproved access, and review identity use reachable through the tunnel. Do not infer success from the option alone.

Exact rules, source requirements, and validation