TIME-SENSITIVE ADVISORY • CHECK FOR UPDATES BEFORE EACH USE

Dated defensive reference. VERIFY LIVE PHP AND VENDOR ADVISORIES BEFORE USE. This 7 November 2026 maintenance edition preserves the original response workflow and consolidates verified 3-7 November vendor, WAF, backport-retention and deployment-verification guidance. Public vendor advisories control fixed-build claims. Investigate possible compromise separately from patch completion; successful PAN-OS exploitation does not establish successful exploitation of every listed vendor product. [S35-S38, S51-S67]

PHP2Shell

MSP EMERGENCY RESPONSE PLAYBOOK

Cross-customer discovery | risk decisions | patching | compromise review | verified closure

Version 1.6 | Updated 7 November 2026 | First published 21 October 2026 | Free operational reference | Editable, unbranded

Incident brief

PHP released upstream fixes for CVE-2026-109618 and CVE-2026-109619 on 21 October 2026 (critical, CVSS v4.0 9.2), covering all web-serving PHP deployment methods including Apache mod_php, FPM, php-cgi, FrankenPHP and LiteSpeed. AWS had observed attempts in honeypots from 17 October. Further evidence documents code execution against vulnerable research honeypots on 24 October. CISA added BOTH CVEs to KEV on 26 October, but its entries do not identify specific compromised production customers. Palo Alto Networks now explicitly reports active exploitation targeting internet-exposed management interfaces. Keep attempts, verified execution, and customer compromise as different evidentiary states. [S1-S3, S12, S24-S26, S29]

The MSP response has two independent objectives: (1) establish the disposition of every reasonably in-scope customer dependency, including vendor-owned services; and (2) confirm remediation and investigate credible indications of exploitation. Updating a server does not retroactively prove that it was uncompromised.

7 NOVEMBER MAINTENANCE | CURRENT VERIFICATION AND LIMITS

Upstream PHP2Shell fixes remain PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12, or proven vendor backports. NCSC-NL software inventory last updated 4 November: 948 tracked products, 185 fixed and 215 vulnerable; entries are product leads, not proof of any particular customer status. Cloudflare updated Free and Managed PHP RCE signatures #2 and #3 on 3 November without changing Block action. [S1-S3, S57-S58]

Supplier-specific changes: Snipe-IT Ubuntu Docker images require v8.8.2 or later, Alpine images v8.8.3-alpine or later; EGroupware official patched images are 26.10.20261021 and 23.1.20261021, with confirmed hosted rollout; Centreon Cloud states its hosted service was patched 22 October while on-premises customers must validate distributor PHP packages. Qualys documented a Windows/macOS assisted upgrade workflow on 4 November; cPanel corrected removal of TuxCare-licensed ELS PHP installations during nightly maintenance on 5 November. [S57, S59-S61]

Security appliance additions: Hillstone advisory HSVD-2026-0113 lists IPS and BDS 6.4.1 and NGFW branch 5.5R12P4.5 as released, with CloudHive/LMS/ADC outstanding on the dated vendor schedule. Singapore CSA lists FortiSOAR/FortiSOAR PaaS running affected versions; use Fortinet PSIRT for exact versions and fixes, not a generic Fortinet assertion. Oracle Security Alert revision 3 is administrative clarification, not proof of a newly issued fix. No additional successful exploitation of these named products is established by these notices. [S62-S65]

Observed malicious requests, WAF blocks, honeypot execution, vendor-reported exploitation and locally confirmed compromise are different evidence levels. PAN-OS active exploitation is documented; do not generalize that confirmation to newly inventoried vendors or to individual customers without corroborating evidence. [S24-S26, S63]

3 NOVEMBER MAINTENANCE | VERIFIED VENDOR DISAMBIGUATION

Broadcom: its ESG advisory 39404 (updated 30 October) identifies Content Analysis and Malware Analysis (CASMA) as AFFECTED by both PHP2Shell CVEs but lists the similarly named Content Analysis (CAS) as NOT vulnerable. Broadcom references CASMA product advisory 39475; its exact affected/fixed build matrix was not publicly accessible in this review. Do not invent a fixed version or close a CASMA dependency without the product-specific notice and implementation evidence. [S51-S52]

F5: K000163821 distinguishes BIG-IP APM access-profile data-plane exposure from BIG-IP Configuration utility control-plane exposure on all modules. Its documented fixes include BIG-IP 17.1.3.7, 17.5.1.11 and 21.1.0.4 for covered maintenance branches. Verify that a device is on the applicable fixed branch or an explicitly supported hotfix; do not apply backend WAF signatures as proof the BIG-IP appliance itself is fixed. [S53]

Siemens: ProductCERT SSA-566512 identifies RUGGEDCOM APE1808 with affected PAN-OS branches as in scope. Siemens instructs customers to install the corresponding available fixed PAN-OS release and contact support for product-specific assistance. Singapore CSA alert AL-2026-157 (3 November) reinforces appliance and management-interface discovery, but is not evidence of a new campaign against CASMA, F5 or Siemens. [S54-S55]

NCSC-NL public repository snapshot (2 November, UTC) tracks 930 products, including 167 fixed, 215 vulnerable, 93 under investigation, 240 runtime-dependent, 214 not affected and one unknown. Treat inventory classifications as dated discovery leads and recheck the manufacturer, not as a substitute for installed-build proof. No newer upstream PHP2Shell source release was identified in the reviewed authoritative sources. [S56,S1-S3]

1 NOVEMBER 2026 CONSOLIDATION | CHANGES AFTER v1.3

Confirmed campaign activity: Unit 42 independently verified the tooling and results reported by Dream Research for exposed PAN-OS management interfaces. Dream reports 24 compromised internet-facing firewalls plus one internal management server, chained with separate kernel CVE-2026-46300. Individual organizations have not been publicly identified. Failed/blocked detections remain distinct from these corroborated campaign findings. [S35-S37]

New vendor coverage: Citrix NetScaler management interfaces; released PAN-OS subbranch hotfixes; Sophos WAF emergency rules; expanded Cisco and NCSC-NL product inventories; Check Point, Broadcom/Carbon Black, TuxCare extended-support backports; Microsoft Azure shared responsibility; and Synology Calendar/Mail Station and PHP updates for legacy DSM branches. [S38-S49]

No new upstream fixed PHP2Shell source versions were identified through this update. Verify fixes against LIVE manufacturer package/advisory matrices. WAF blocks and CISA KEV inclusion do not themselves establish installation or a specific customer compromise. [S1-S3,S43-S45]

27 OCTOBER UPDATE | VERIFIED DECISIONS SINCE VERSION 1.2

CISA KEV: CISA lists BOTH CVE-2026-109618 and CVE-2026-109619 as known exploited (added 26 Oct 2026), forensicTriage=Yes and dueDate=29 Oct 2026 under its federal directive framework. This date is NOT a general private-sector MSP compliance deadline. Record any contractual or regulatory requirements separately. CISA classification does not prove a named client was compromised. [S24]

Active attack assessment: 24 Oct honeypot research documents 35 Apache-child shell executions across three intentionally configured PHP 8.4.26 mod_php honeypots; this is successful RCE on controlled sensors, not 35 victim organizations. The evidence is consistent with CVE-2026-109618 and does not independently demonstrate the distinct CVE-2026-109619 path. Palo Alto changed its advisory to state that active exploitation has been observed targeting its exposed management interface. Do not infer a confirmed PAN-OS customer compromise without per-asset investigation. [S25-S26]

Vendor updates: Palo Alto now rates its affected PAN-OS/Panorama management interface issue CRITICAL (9.2), urgency HIGHEST, and has released multiple hotfixes while other branches remain scheduled. Tenable Security Center / Enclave Security patch SC-202610.2 is available (23 Oct). Peplink ICVA 2.14.4 and selected Balance/MAX Edge Computing special firmware 8.6.1s042 are available; verify model and hardware revision. Official PHP Windows -1 rebuilds address a separate Brotli CVE. [S25, S27-S30]

23 OCTOBER UPDATE | DECISIONS THAT CHANGE THE RESPONSE

23 OCTOBER EVIDENCE BASELINE: Retrospective review should begin no later than 17 October for exposed assets when logs permit. Sophos corrected its earlier success claim to failed/blocked attempts; Arctic Wolf did not confirm payload execution. These corrections must remain in the record alongside newer, separately sourced honeypot code-execution evidence and CISA KEV listing. [S12, S17-S18, S24, S26]

Vendor changes: CloudLinux now reports all fixed alt-php and ea-php builds in stable and upstream-numbered packages for branches 8.2-8.5. Earlier documented backports can already be fixed. CloudLinux corrected its earlier advice: keep the ELS ALT PHP (php-els) repository enabled if installed. Cisco identifies Expressway, Expressway Select, Ultra-Reliable Wireless Backhaul and Duo Access Gateway as affected, with different fixed-release availability. Recheck cPanel, Plesk and Palo Alto notices by exact product/build. [S4-S5, S11, S13, S19-S21]

Exploit and adjacent advisory: VulnCheck reports laboratory RCE for CVE-2026-109618 on mod_php PHP 8.4.10-8.4.26 and 8.5.10-8.5.11 on AMD64/ARM64 with production-style defaults; this does not demonstrate a compromised customer. PHP also published a 23 October informational advisory for distinct CVE-2026-115560 involving an unusual session serialization configuration. Keep session.upload_progress.enabled=0 until the next regular fix if following PHP mitigation guidance; apply PHP2Shell patches regardless. [S20, S22-S23]

Affected branch	Upstream fixed release	Important qualification
PHP 8.5	8.5.12	Also verify the running web-serving worker.
PHP 8.4	8.4.27	Windows NTS and TS packages differ.
PHP 8.3	8.3.36	Vendor packages may use backported fixes.
PHP 8.2	8.2.35	PHP project support ends 31 Dec 2026.
PHP 8.1 and older	No PHP project release	Use verified supported vendor backport or upgrade.

Source: PHP Security Team [S1]. The table concerns upstream fixed releases. A vendor-maintained package can be fixed without changing the upstream version string. Never infer patch status from a single version command.

As of 1 November, PHP2Shell upstream fixed source versions remain unchanged. Official Windows -1 rebuilds issued 26 October for these versions address a SEPARATE bundled Brotli issue, not a new PHP2Shell source fix. Treat CVE-2026-115560 (session handling) and CVE-2026-111497 (Brotli) as separate assessments. An older vendor-verified backport can be fixed despite an older displayed PHP version. [S1, S23, S30]

Immediate response sequence

Window (guidance)	Action	Required evidence
First 60 minutes	Assign incident owner; establish customer scope; issue initial notice; pull authoritative sources.	Response ticket, owner, customer universe, advisory snapshot.
First 4 hours	Identify internet-exposed PHP and critical vendors; assign P0/P1 priorities; approve changes.	Asset leads, ownership, exposure and authorization records.
First 24 hours	Apply available patches or isolate; validate workers; hunt on exposed assets.	Before/after runtime evidence, change tests, investigation notes.
Until closure	Resolve unknowns, vendor dependencies and exceptions; send customer dispositions.	Verified status for every in-scope asset or documented open risk.

These are operational targets, not regulatory deadlines. Adjust to contracts, risk, staffing and evidence. Suspected compromise triggers incident response at any point.

1. Activate and govern the response

1.1 One response, separate customer records

1. Open one master vulnerability response record. List every customer in scope, including those requiring only third-party dependency validation.
2. Assign an incident coordinator, discovery lead, remediation lead, threat-hunting lead, customer communication owner and quality reviewer. Small teams may combine roles but should separate execution from verification where practical.
3. Confirm emergency-change authority for MSP-owned and customer-owned systems. Document downtime approval, maintenance constraints and sign-off requirements.
4. Define a second track for possible incidents. A vulnerable system is not automatically compromised; credible indicators merit incident-response escalation.
5. Record factual updates with timestamp, source and owner. Maintain a decision log for exceptions and disputed ownership.

6. Record both CISA KEV entries, dated source and whether its forensic-triage and federal due-date requirements apply to each customer. Private-sector urgency is driven by business risk and applicable agreements, not a universal KEV deadline. Escalate suspected exploitation before destructive changes. [S24]

1.2 Responsibility and decision gates

Gate	Owner	Pass requirement
G1 Scope accepted	Response coordinator	Customer roster, managed scope, delegated services and unknowns recorded.
G2 Exposure assessed	Discovery lead	Each lead has evidence, owner and status; negatives have bounded scope.
G3 Change authorized	System/customer owner	Patch, isolation or exception has explicit approval.
G4 Patch verified	Independent reviewer	Serving runtime, workers and application function confirmed.

Gate	Owner	Pass requirement
G5 Compromise disposition	Security lead	Threat-hunt results documented or escalated to IR.
G6 Customer closure	Account owner + coordinator	Residual risks, vendor dependencies and customer notice complete.

Stop conditions: no authority to change a system; suspected compromise requiring preservation; unverified patch source; material application outage risk; or ambiguous evidence that could create a false “safe” conclusion. Escalate rather than bypassing the gate.

2. Define the customer exposure universe

2.1 Investigate all four dependency classes

Class	Include	Control question
MSP-owned	Internal portals, RMM/PSA adjacent tools, monitoring, hosting, management UIs, dev systems.	Does this create cross-customer access or shared service exposure?
Customer-owned	Websites, intranets, internal apps, business systems, desktops running local services.	Is it in our support or advisory scope?
Cloud and containers	VMs, images, pods, managed runtimes, serverless functions, registries, CI/CD templates.	Who can rebuild and redeploy the underlying runtime?
Third-party	Website agencies, hosting panels, appliances, SaaS vendors and embedded PHP dependencies.	Who must attest to a fix, and how do we verify?

Include embedded PHP in security-management interfaces and vendor appliances even if the customer has no standalone PHP server. Specifically assess Palo Alto PAN-OS/Panorama management, Tenable Security Center and Enclave Security, Peplink InControl Virtual Appliance (ICVA), and Balance/MAX routers only where Edge Computing is enabled, in addition to the previously listed Cisco products. [S25, S27-S29]

28-31 OCT DEPENDENCY EXPANSION

Add firewall and ADC management interfaces, including internet-reachable PAN-OS/Panorama UI or XML API, dataplane management profiles, Citrix NetScaler NSIP/management-enabled SNIP/cluster IP, Check Point security portals and WAN/edge appliances. Inventory identity integrations, upstream management servers, and all devices that can store VPN/LDAP/AD credentials. [S35,S36,S38-S40,S48]

Include Synology NAS devices: DSM release, Package Center PHP package(s), Calendar and Mail Station versions, installed PHP-dependent Web Station/WordPress/phpMyAdmin or other apps, and publicly reachable services. Synology states its built-in DSM PHP is not externally exposed; classify deployed applications separately. Hyper Backup and Synology Drive are NOT PHP2Shell-affected according to Synology. [S46-S47]

Add Azure Linux App Service release channel, Windows custom PHP, customer images and custom containers to the cloud dependency inventory. Record the party responsible for runtime upgrades. [S45]

3 NOVEMBER APPLIANCE DISCOVERY: Split Broadcom CASMA from CAS in the asset inventory, and do not collapse either into a generic "Content Analysis" record. For F5, record BIG-IP module/license, software branch, Configuration utility reachability and APM access-profile enablement separately. For Siemens,

record RUGGEDCOM APE1808 model and the actual PAN-OS image installed on the device. Use vendor advisory revisions and current fix availability, not vendor family names alone. [S51-S56]

7 NOV EXPANDED DEPENDENCY DISCOVERY

Record administrative and embedded PHP dependencies including Hillstone IPS/BDS/NGFW and other listed appliance families, FortiSOAR/FortiSOAR PaaS, affected Oracle products, Centreon, EGroupware and Snipe-IT. Product naming alone is not enough: collect exact vendor/build/branch, management reachability, hosted vs customer-operated responsibility, runtime ownership and actual running image/handler. [S57, S59-S65]

2.2 Correlate discovery sources

Start with RMM inventories, EDR software discovery, vulnerability platforms and CMDB data. Reconcile against DNS/domain records, cloud control planes, public-facing application inventory, web hosting panels, network exposure maps, container catalogs, procurement/vendor lists, backup catalogs and tickets referencing PHP, WordPress, Drupal, Joomla or Magento. [S7-S8]

Flag unmatched applications and asset groups as UNKNOWN. An inventory source that finds no PHP cannot prove PHP is absent. Shared-hosting control panels, vendor appliances and self-contained application stacks are frequent blind spots.

7 NOV ADDITIONAL INVENTORY EVIDENCE

For Windows include every standalone PHP installation, IIS FastCGI mapping, service binary path, package flavor (TS/NTS, architecture), and supported remediation owner. For macOS identify Homebrew versus MacPorts/MAMP/manual installations; the published Qualys automation only covers Homebrew-managed macOS PHP. For containers capture immutable image digest, base OS, PHP package provenance, deployed tag and running container identity. For appliances capture management interface ACL, firmware/hotfix and approved vendor patch source. [S59-S62]

2.3 Minimum per-asset record

Field group	Record
Identity	Customer ID; asset/service ID; hostname/domain; application name; production/development.
Technical	Web-serving PHP executable/module/image; SAPI; version; package release; OS; network exposure.
Management	MSP/customer/vendor owner; administrative authority; critical business process; change window.
Assessment	Discovery evidence; exact advisory/vendor source; risk class; suspected compromise review.
Remediation	Change ticket; approved option; before/after version; restart evidence; functionality checks.
Closure	Reviewer; UTC verification time; immutable evidence link; exception or open dependency.

3. Discover PHP without disturbing production

Use locally authorized, read-only collection first. Do not run internet-facing exploit probes, proof-of-concept payloads, aggressive port scans or arbitrary binaries to establish exposure. Limit evidence collection to the customer and systems you are authorized to administer.

3.1 Windows, IIS and local application stacks

Check installed software and packages, known PHP paths, services, running processes, IIS FastCGI mappings, IIS site/application pool settings, web server configuration and any application-specific PHP stack. A CLI version can differ from the runtime serving a web request.

```
Get-Command php.exe -All -ErrorAction SilentlyContinue
Get-CimInstance Win32_Process | Where-Object { $_.Name -match
  '^(php|php-cgi|httpd|nginx|w3wp|iisexpress)\.exe$' } |
  Select-Object Name,ExecutablePath,ProcessId
Get-NetTCPConnection -State Listen | Select-Object LocalAddress,LocalPort,OwningProcess
```

For IIS, review FastCGI application mappings and the absolute executable path. If PHP runs via an embedded module or separate service, verify that instance too. If a service listens only on 127.0.0.1 or ::1, record reduced network exposure, not automatic immunity. A local process could still consume untrusted input.

Companion script: Windows-PHP-Discovery.ps1. It records leads without invoking discovered executables. Its negative result is NOT proof of absence. Keep resulting path and host data confidential.

3.2 Linux packages, services and workers

```
command -v php && php -v
ps -eo pid,user,args | grep -E '[p]hp-fpm|[p]hp-cgi|[l]sphp|[a]pache2|[h]ttpd'
dpkg-query -W -f='${Package} ${Version}\n' 'php*'  # Debian family
rpm -qa | grep -E '^(php|ea-php|alt-php|plesk-php)' # RPM family
```

Read the package vendor changelog and security update notes. Map each virtual host to the actual PHP handler, pool, module or binary. Check old workers after package updates. Distribution backports require package-level proof, not upstream version comparison alone. [S1]

Companion script: Linux-PHP-Discovery.sh. Validate from service configuration and vendor advisory before assigning a final status.

3.3 Containers, orchestrators and PaaS

```
docker ps --format '{{.Names}} {{.Image}}'
kubectl get pods -A -o wide   # on authorized clusters only
```

Inspect Dockerfiles, pinned base image digests, container contents, lockfiles, registries and runtime build manifests. A host package update does not change an already built container. Rebuild using fixed sources, redeploy, replace old replicas and verify the running image digest and in-container runtime.

3.4 Managed hosting, control panels and appliances

cPanel/WHM: check the panel build separately from each domain-selected EasyApache4 handler. Previously published fixed cPanel & WHM builds include 110.0.153, 134.0.66, 136.0.50 and 138.0.18; verify the LIVE cPanel matrix. Plesk: check shipped PHP handlers AND sw-engine/plesk-engine, including backports whose displayed versions did not change. CloudLinux: distinguish native PHP, ea-php and alt-php, and verify exact package release, repository origin and running PHP workers. [S4-S5, S11, S19]

Vendor appliances: include PAN-OS/Panorama management UI/XML API (including dataplane management profiles), Citrix NetScaler ADC/Gateway, Cisco Expressway/Expressway Select, Duo Access Gateway, ISE Portal Builder, URWB and Unified Industrial Wireless, Check Point security portals, Carbon Black App Control and Synology PHP-based apps. Use the LATEST vendor advisory for fixed release, authorization prerequisite and interim control. The 23 October Cisco ETA examples are superseded by v1.10 on 30 October. [S38-S49]

27 OCT EMBEDDED-VENDOR SCOPE: Palo Alto Networks identifies the management HTTPS UI/XML API as affected, including dataplane interfaces configured with a management profile. GlobalProtect portals and gateways are not affected by these CVEs. Inventory the exact PAN-OS maintenance branch, hotfix and management-plane reachability; Panorama is also within scope. Tenable Security Center <= 6.9.1 and Enclave Security <= 1.9.1 require product patch verification. Peplink: check ICVA <= 2.14.3 and Edge Computing on Balance/MAX running firmware 8.6.1 GA; feature is off by default. Peplink-hosted InControl 2 is unaffected. [S25, S27-S29]

Embedded management components and inherited runtimes

For appliances managed by providers, request exact vendor notice and evidence for the specific release. Record approved management-plane access, alternate paths, external reachability and repair owner. Examples: NetScaler ADC/Gateway; PAN-OS/Panorama; Cisco Expressway, Duo and ISE Portal Builder; Check Point; Carbon Black App Control; Synology NAS; and affected VoIP/legacy PHP appliances in the NCSC inventory. [S38-S42,S46,S48-S49]

Broadcom product-name check: verify CASMA versus CAS by exact full product name, manufacturer ID, and running appliance build. Broadcom ESG advisory 39404 categorizes CASMA as affected and CAS as not vulnerable. If CASMA is present, obtain the access-controlled CASMA advisory 39475 or written Broadcom support determination covering the installed release before declaring "patched" or "not affected." Do not infer exploitability from any one scanned endpoint. [S51-S52]

F5 BIG-IP: separately inventory the APM access-profile data plane and the Configuration utility administrative control plane. Record configured management interface allowlists, exposure history, BIG-IP branch and exact fixed update (17.1.3.7, 17.5.1.11 or 21.1.0.4 for applicable branches). F5 BIG-IQ Centralized Management and F5 Insight are reported not vulnerable in the reviewed advisory; do not generalize BIG-IP findings to them. [S53]

Siemens industrial edge: RUGGEDCOM APE1808 is affected when running relevant PAN-OS releases. Check the installed PAN-OS version, reachable management ports/paths and any documented industrial change-window constraints. Obtain the Siemens product notice and corresponding Palo Alto fixed-build applicability; do not infer that all Siemens products are affected. [S54]

Expanded priority: exposed administrative surfaces and post-patch investigation

Classify internet-accessible, previously vulnerable PAN-OS management interfaces as urgent remediation AND incident-investigation leads, including interfaces patched after the exposed interval. Unit 42 independently confirmed the reported intrusion campaign. Investigate for persistence, root access and downstream credentials; customer-specific compromise still requires evidence. [S35-S37]

For NetScaler management IPs, Check Point portals, Synology PHP-serving apps and other appliance management interfaces, prioritize actual exposure and vulnerable versions rather than the presence of PHP alone. Restrict or isolate management services while completing fixes. For Sophos WAF, Cloudflare or Citrix backend WAF signatures, record separate mitigated status, not patched status. [S39-S44,S46]

7 NOV HOSTING AND APPLIANCE EXCEPTIONS

Hosted and self-hosted deployments must be separated. EGroupware and Centreon hosted-service confirmations do not patch customer-operated instances; for Snipe-IT verify Alpine versus Ubuntu container lineage and the image deployed, not merely a general version label. A vendor status of "under investigation" or a national CSIRT affected-product listing must be matched to current vendor affected-version and fixed-release documentation. [S57, S60-S64]

4. Classify risk and establish remediation order

Use the operational priority matrix below with the 26 October CISA KEV status for BOTH CVEs. Record internet reachability, SAPI, exact vendor build, exploit prerequisites, worker privileges, secrets, administrative authority and isolation options. Palo Alto now rates internet-exposed PAN-OS management PHP2Shell CRITICAL (9.2), urgency HIGHEST, and explicitly reports active exploitation targeting those management interfaces. Give exposed, unpatched management planes and vulnerable mod_php elevated attention. Other devices, including Cisco URWB, may have different authentication requirements. An attack indicator is not by itself confirmed local command execution. [S20-S21, S24-S26]

Priority	Decision rule	Required action
P0	Unpatched internet-facing web-serving PHP; especially Apache mod_php or high-impact shared infrastructure.	Patch or isolate immediately under emergency change authority. Initiate focused hunt.
P1	Unpatched web-serving PHP behind VPN, partner connectivity, broad internal access or high-value data.	Expedited change; reduce reachability and inspect logs.
P2	Restricted internal web service or non-production runtime with credible untrusted request path.	Schedule urgent patch and verify access boundary.
P3	CLI-only PHP used for known local tasks with no web-serving SAPI or untrusted input path.	Patch under expedited process; assess execution context.
UNKNOWN	Version, actual runtime, scope or vendor patch status cannot be established.	Keep open, assign owner and deadline; do not label unaffected.

Highest confidence is not always highest priority. An exposed app with uncertain software inventory is an urgent discovery problem. Risk can rise further if the web worker accesses customer databases, API secrets, network shares, backup systems or adjacent tenants.

Investigation evidence categories: (A) scans/no verified payload; (B) credible attempt; (C) blocked/failed attempt; (D) successful RCE on a controlled research honeypot, not the customer asset; (E) process-correlated RCE on the customer asset; (F) confirmed local persistence, data access or lateral activity. For CISA KEV status and Palo Alto observed attack targeting, record source and advisory date in a separate threat-context field. Never mark an individual customer compromised solely because its product is in KEV or it was attacked elsewhere. [S24-S26]

3 NOVEMBER PRIORITY RULE: Treat confirmed CASMA assets with unknown patch availability as open, vendor-dependent exposure assessments requiring a named owner and risk decision. Prioritize F5 BIG-IP Configuration utility access from untrusted networks and relevant BIG-IP APM exposure by the applicable vendor conditions. RUGGEDCOM APE1808 management services inherit PAN-OS-specific risk only if that product is running an affected PAN-OS version. CSA 3 November reporting confirms broader vendor product scope, not successful exploitation of each named platform. [S51-S55]

5. Remediate safely

5.1 Patch selection and provenance

1. Obtain packages from the official PHP project, OS distribution or supported product vendor. Avoid unauthenticated third-party mirrors and unreviewed public fixes.

2. For upstream PHP2Shell fixes, use PHP 8.2.35, 8.3.36, 8.4.27 or 8.5.12 on the corresponding supported branch. For older branches, verify a vendor-supplied backport for BOTH CVEs or upgrade to a supported branch. The separately disclosed CVE-2026-115560 is NOT documented as fixed by these 21 October releases. [S1, S19, S23]
3. Confirm application prerequisites: extensions, TS/NTS builds on Windows, PHP-FPM pool settings, opcache, INI hierarchy, web-server modules, runtime image base, application tests and rollback package.
4. Take backups or snapshots according to the customer change policy. Preserve important evidence before rebooting if compromise is suspected.
5. Apply patch with approved change tooling; restart or replace ALL affected workers/containers; validate actual web-serving runtime and functionality.
6. Record installed package ID or file build, worker restart time, functional-test output and a second-party verification result.

CLOUDLINUX REPOSITORY CORRECTION: CloudLinux status update of 23 October 21:36 UTC supersedes an earlier disable instruction. If you added the ELS ALT PHP (php-els) repository, KEEP IT ENABLED. Check cloudlinux-release currency, the cl-ea4 repository on cPanel, and regular package updates when yum/dnf returns "Nothing to do". The status page and applicable support article must be consulted together; follow the latest status correction. [S19]

CLOUDLINUX 23 OCT FIX STATUS: CloudLinux reports all supported alt-php and ea-php fixed packages in stable, including version-aligned alt-php82/83/84/85 8.2.35-1 / 8.3.36-1 / 8.4.27-1 / 8.5.12-1 and ea-php82/83/84/85 with the same upstream-aligned version numbers. An earlier CVE-backported package may already be protected. Use installed package release and vendor changelog/rebase evidence, not php -v or security-only update filters alone. CloudLinux reports native fixed builds in stable for all its affected streams as of 22 October 19:50 UTC. [S19]

VENDOR PATCH VERIFICATION BASELINE: Tenable Security Center / Enclave Security product patch SC-202610.2 (embedded PHP 8.2.35) and Peplink ICVA 2.14.4 / model-specific 8.6.1s042 Edge Computing fixes require product-level installation evidence. PAN-OS patch status has advanced since 27 October: use the updated 29 October fixed-build matrix in Appendix B and live Palo Alto advisory. Separate PHP2Shell from the Brotli patch caveat on PAN-OS 11.2.10-h16. [S27-S29,S38]

New vendor patch-selection requirements (28-31 October)

PAN-OS/Panorama: Consult branch-specific released hotfix thresholds in the 29 Oct Palo Alto advisory, not the earlier 27 Oct ETA list. The PHP2Shell fix and separate Brotli CVE-2026-111497 differ on PAN-OS 11.2.10-h16 (PHP2Shell only); 11.2.10-h17 covers both. The general solution matrix applies to PA-Series, VM-Series and Panorama. Check exact subbranch, download, installed version and advisory revision. [S38]

Citrix NetScaler ADC/Gateway: fixed releases are 14.1-73.49+, 13.1-64.32+; ADC 14.1-FIPS 14.1-73.49 FIPS+; ADC 13.1-FIPS/NDcPP 13.1.37.286+. Confirm branch and management-interface accessibility; NetScaler Console is listed unaffected. [S39-S40]

Cisco advisory v1.10 (30 Oct): Expressway/Select fixed 15.5.21; Duo Access Gateway fixed 3.2.0; ISE Portal Builder fix deployed (vendor states no customer action). Wireless remediation varies by product; use current Cisco bug/advisory release line and authentication prerequisite rather than 23 Oct release estimates. [S42]

TuxCare: patched backports exist across alt-php branches, but OS-level ELS and separate ELS for PHP subscriptions cover different packages. A fixed old-version string may have a higher release suffix. Verify subscription, vendor repo, exact rpm/deb release and BOTH CVEs; third-party packages are not automatically covered. [S44]

Synology: use DSM-family-specific Calendar, Mail Station and PHP package builds in Appendix B. PHP 7.3 has no Synology fix. Mail Station requires a separate MANUAL Package Center update. Confirm affected app service restarts and accessible routes, not DSM version alone. [S46-S47]

Other embedded products: Check Point, Carbon Black App Control, Citrix and GetPageSpeed/legacy distribution builds appear in NCSC-NL inventory. Treat list entries as discovery leads; the exact vendor advisory and installed product build control closure. [S48-S49]

3 NOVEMBER PRODUCT FIX SELECTION | SPECIFIC VENDOR PROOF

Broadcom CASMA: affected per Broadcom ESG advisory 39404. The publicly accessible umbrella advisory does not disclose exact CASMA fixed release(s). Obtain CASMA-specific advisory 39475 through authorized Broadcom support, match the customer hardware/software version, confirm the released vendor fix and retain the change record. Broadcom Content Analysis (CAS) is listed NOT vulnerable to these two CVEs; record that determination separately. [S51-S52]

F5 BIG-IP: vendor K000163821 lists fixed releases 17.1.3.7, 17.5.1.11 and 21.1.0.4 for the applicable supported branches, with vendor-specific engineering hotfix alternatives referenced in that advisory. Confirm exact source release and whether the configuration utility and/or APM access profile is enabled and exposed. Do not assume a WAF rule for backend pool members patches F5 control-plane PHP. [S53]

Siemens RUGGEDCOM APE1808 running PAN-OS: follow SSA-566512 and the applicable Palo Alto PAN-OS branch/fixed-release matrix. Siemens explicitly directs customers to support for patch details. Verify that the fixed PAN-OS release is approved and installed on the specific APE1808 deployment; if unavailable, document management-plane isolation as an interim exception. [S54]

7 NOV PATCH PROVENANCE AND PERSISTENCE

cPanel 5 November correction CPANEL-58351: release notes for branches 110.0.155, 134.0.68 and 138.0.21 state nightly maintenance no longer removes TuxCare ELS PHP installed with a TuxCare license key. Other branches require direct confirmation. Verify the underlying TuxCare package and both-CVE backport evidence, assigned PHP handler, and package persistence after subsequent maintenance. The defect does not alone prove that a customer ran a vulnerable PHP runtime. [S61]

Snipe-IT: verify official Ubuntu image v8.8.2 or later versus Alpine image v8.8.3-alpine or later, including deployed digest; EGroupware: check official 26.10.20261021 / 23.1.20261021 images and live PHP 8.5.12. Centreon on-premises: obtain corrected PHP packages from distro/provider and verify the active runtime after restarting relevant services. [S57, S60]

Hillstone: IPS 6.4.1, BDS 6.4.1 and NGFW 5.5R12P4.5 are listed released in HSVD-2026-0113. Verify each branch independently; CloudHive/LMS fixes were scheduled for 9 November and ADC for 15 November as of this release, not yet presumed available. FortiSOAR and FortiSOAR PaaS: follow current Fortinet product PSIRT for exact affected ranges and supported patches. Oracle product fixes must be validated by exact supported release and support document. [S62-S65]

Qualys TruRisk Eliminate CAR (4 November): its documented script library item "PHP Update to Latest Patch Version" supports Windows and Homebrew-based macOS upgrades to latest patch of existing minor series, via agent or authenticated scanner; Windows flow verifies official archive SHA256 and rolls back on verification failure. It stops for EOL branches and is not a license to overwrite embedded/vendor-managed PHP or to run untested binary replacement on production. Qualys temporary mitigation scripts reduce exposure, not repair these CVEs. [S59]

5.2 Interim measures when patching is blocked

No generic configuration mitigation completely repairs PHP2Shell. Isolation or tightly restricted network access is preferable when a fixed package is unavailable. Cloudflare states managed WAF protections were enabled by default on 21 October and describes request-plus-response inspection; Imunify360 published rules targeting known upload-progress exploit patterns. Validate enabled rules, origin-bypass risk, observed matches and application impact. WAF blocks are not confirmation of successful customer compromise. [S1, S6, S11]

PAN-OS management mitigation: limit access to trusted internal addresses or a tightly controlled jump host. Palo Alto threat signatures only apply to management traffic if it traverses an inspected dataplane path, with the required inbound management TLS inspection, replacement certificate and Threat Prevention policy. Do not credit signature availability as protection when these conditions are absent. Peplink ICVA: restrict TCP/4443 management to VPN/management VLAN; for affected Edge Computing routers, disable WAN web administration and temporarily disable or isolate ContentHub. Treat each control as temporary until fixed firmware is installed and verified. [S25, S29]

PHP temporary controls target specific paths and can affect application availability. The PHP project recommends session.upload_progress.enabled=0 applied before request parsing, with every worker restarted; do not rely on request-time ini_set() or FPM .user.ini. On 23 October it separately advised keeping this disabled until the next regular bugfix release for CVE-2026-115560 under unusual session-serializer switching conditions; this is NOT a third PHP2Shell CVE. Other partial measures include controlled memory_limit=-1, request-size constraints and PHP 8.5 fatal_error_backtraces=0. None substitute for PHP2Shell patching. [S1-S3, S23]

Exception owner must approve affected application, business impact, interim control, test result, evidence, expiration date, escalation trigger and planned permanent remediation. Label such systems TEMPORARILY MITIGATED, never PATCHED.

Enhanced controls and caveats

Cloudflare updated PHP2Shell detection expressions on 28 and 30 October in Managed/Free and response rulesets, retaining blocking actions. Verify that applicable rules are active, have no overrides and actually cover the route/origin. Do not equate a WAF event with code execution. [S43]

Sophos Firewall v22/v23 WAF common-threat-filter hotfix (28 Oct): the application-attacks rules work only when the WAF rule has a protection policy assigned, CTF enabled and the application-attacks group active. For false-positive review see reverseproxy.log rule IDs 9481021, 9481022 and 9481023. This is not a PHP patch. [S41]

Citrix WAF signature 186 protects backend PHP apps; do not treat it as proven protection of NetScaler management interfaces. Isolate NSIP, management-enabled SNIP and cluster management access, and confirm the exact NetScaler firmware. [S39-S40]

Microsoft (30 Oct): managed Azure built-in PHP runtimes were updated for stated Linux services; customer-managed Windows PHP, unsupported branches, custom containers and images remain customer responsibilities. On App Service Linux Extended channel, select Standard/Latest; App Service for Windows built-in PHP is end of life. Rebuild and redeploy custom images. [S45]

CASMA / F5 / Siemens interim controls: restrict or isolate susceptible administrative interfaces when exposed, using manufacturer-approved access controls and business-authorized change procedures. For F5 BIG-IP APM, document data-plane access-profile exposure separately from the control-plane Configuration utility. For Siemens APE1808, use the PAN-OS and Siemens guidance for management-access restrictions.

Treat backend WAF and appliance controls as distinct; neither supplies evidence that PHP2Shell is patched. [S52-S55]

7 NOV WAF UPDATE AND SAFE TEMPORARY CONTROLS

Cloudflare 3 November updates improved PHP2Shell detection expressions for signatures #2 and #3 in its Free and Managed rulesets; documented action remains Block. Confirm these rules are enabled for the relevant route, have not been overridden or bypassed, and collect origin evidence for any alert. WAF matches do not demonstrate successful code execution, and WAF does not replace runtime patches. [S58]

Until approved security appliance firmware can be installed, restrict administrative/management interfaces to trusted networks or controlled jump hosts. Preserve evidence of any previous internet exposure. Validate operational impact and schedule a verified patch; do not mark a host patched based solely on access restrictions. [S62-S64]

6. Verify the actual serving runtime and restore service

6.1 Mandatory verification sequence

1. Identify exact installed package/binary path, repository and vendor release. Verify a fix for BOTH CVE-2026-109618 and CVE-2026-109619. CloudLinux ea-php and alt-php may have a backport at an older apparent PHP version; consult the exact RPM changelog. For rebase builds that omit the CVE ID in the changelog, compare the vendor-documented fixed package release/branch. Older Plesk backports can retain a version number but differ by build date. Confirm the LATEST CloudLinux ELS repo correction, cloudlinux-release and cl-ea4 state. [S4-S5, S19]
2. Map the application request handler to its PHP binary, module, pool or container. Checking “php -v” alone is not enough.
3. Confirm every old PHP worker/process was stopped or replaced. Check old container replicas, scheduled app pools, long-lived FPM workers and stale module loads.
4. Confirm approved PHP INI and extensions load, and test critical application routes. Check login, data access, uploads, APIs, scheduled jobs and error logs as applicable.
5. Verify access restrictions/WAF remain enabled and no emergency rule broadens access unexpectedly.
6. Collect independent review evidence. A successful package install without a serving-runtime check is PATCHED - UNVERIFIED.

7. Record whether the temporary mitigation session.upload_progress.enabled=0 is enforced at the correct configuration layer, and verify actual worker effective settings if mitigation is still needed for CVE-2026-115560. Keep separate patch compliance for the two PHP2Shell CVEs and follow the later PHP advisory for the distinct issue. [S23]

8. For embedded systems record product name, model/hardware revision, branch/maintenance train, installed hotfix, vendor download availability, management exposure, before/after active firmware, restart/commit proof and independent post-change test. A listed release or published ETA is not a completed customer patch. For PAN-OS 11.2.10 document whether the separate Brotli fix is included in the chosen build. [S25, S27-S30]

Expanded verification evidence for embedded systems

Capture installed product/build, update transaction, service/appliance reboot or worker replacement, verified serving build, management reachability after hardening, current WAF rule/policy settings and vendor fixed-build advisory. Separate PHP2Shell patch evidence from kernel CVE-2026-46300 and Brotli CVE-2026-111497 verification. [S35-S46]

For Synology, capture DSM version, every relevant Package Center PHP build and application version, successful manual Mail Station update when installed, and service functionality. For CloudLinux/TuxCare backports, retain the full repository, package release and backport statement, not only php -v. [S44,S46]

3 NOVEMBER VERIFICATION: For CASMA, do not close remediation until the customer-specific Broadcom advisory or manufacturer confirmation gives an applicable fixed build and the running image is verified. For BIG-IP, capture running TMOS version, APM/Configuration utility scope, fixed release or supported hotfix proof, restart/reload status as recommended by F5, and functional checks. For RUGGEDCOM APE1808, capture its PAN-OS branch/hotfix, Siemens applicability statement and live management reachability. A scan finding alone is insufficient. [S51-S54]

7 NOV MANDATORY ADDITIONAL CHECKS

Post-change reviewer must inspect loaded worker version and process identity, restart date/time, handler mapping, container digest or appliance firmware, and application health. On TuxCare/cPanel ELS hosts, perform a post-nightly-maintenance package and handler persistence check. For Qualys remediation retain the CAR job and rollback result, but independently confirm the live PHP worker. Hosted services require dated provider attestation and scope statement. [S59-S61]

6.2 Evidence bundle

Before	After	Security / business disposition
Host, runtime, version, SAPI, exposure and timestamp.	Patched package or version; active worker/image proof; restart timestamp.	Compromise hunt scope and outcome.
Change approval and backup/rollback method.	Application test outputs and observed availability.	Customer approval or exception and notice.
Provider advisory and package identification.	Reviewer identity and UTC verification time.	Residual risk, external dependencies and recheck due date.

Do not expose a public phpinfo() diagnostic page to establish versions. Prefer authorized admin configuration, server-side logs and temporary authenticated checks that are removed immediately afterward.

7. Check for attempted or successful exploitation

Hunting must be independent of patch verification. AWS observed attempts beginning 17 Oct. Sophos later corrected its own unsuccessful attempts; Arctic Wolf did not prove remote payload execution. Research published 24 Oct documents 35 shell executions on three intentionally configured PHP 8.4.26 mod_php honeypots; this confirms successful command execution in controlled sensors, not customer compromises. CISA added BOTH CVEs to KEV 26 Oct, and Palo Alto reports observed active exploitation targeting internet-exposed management. Establish local outcome using raw evidence and preserve volatile data before restarting suspect systems. [S12, S17-S18, S24-S26]

7.1 Scope and timeline

Review at least 17 October 2026 onward where logs permit; go earlier if local evidence indicates. Correlate multipart/request metadata, PHP OOM and cleanup messages, web-worker PID and crash records, child-process creation, outbound requests and authentication changes. For exposed PAN-OS/Panorama management, preserve vendor-appropriate management and threat logs and monitor for unexpected config/API activity. Record telemetry gaps, timestamp basis and evidence state; do not transform CISA KEV entry, a WAF signature, a honeypot shell or Palo Alto targeting statement into an assertion that your customer was compromised. [S12, S24-S26]

7.2 Hunt checklist

Telemetry	Investigation hypothesis	Caution
Web/reverse proxy logs	Bursts of POST/multipart activity, excessive fields/parts, missing usable Content-Length, unusual errors.	Patterns may be benign; raw logs may omit critical request body detail.
PHP / web service logs	Out-of-memory fatals, crashes, worker churn, repeated early warnings or timeouts.	No error does not establish safety.
EDR / process telemetry	Web worker spawning shells/utilities; abnormal child processes.	Review application maintenance tasks before declaring compromise.
File/config changes	Unexpected PHP files, session artifacts, auto_prepend_file changes, persistence.	Compare with deployments; preserve hash and timestamp metadata.
Network / identity	Unusual egress, credential use, lateral access from worker identity.	Correlate with business workflow and account scope.
WAF / CDN	Matching php2shell protection rules, action, origin response and source context.	WAF detection is a lead, not a confirmed exploit.
AWS MadPot retrospective signal	Review 17 Oct onward for POST multipart forms containing PHP_SESSION_UPLOAD_PROGRESS; correlate sender, path, worker, response, EDR and time.	Body fields may not be logged. AWS IP indicators may be shared anonymization infrastructure; investigate context, do not treat an IP match as proof. [S12]
Sophos attempted Potassium staging	Correlate suspicious multipart POST activity with web-worker child processes, download commands, attempted /tmp staging, and associated IP/domain/hash indicators published by Sophos.	Sophos withdrew its success claim. A network or hash match is context to investigate, not proof of malware execution. [S17]
Arctic Wolf second-stage attempts	Review padded upload fields and attempted fetches from 92.118.112[.]100 with independent process/file and network evidence.	Payloads on hosting infrastructure do not prove that the targeted PHP host downloaded or executed them. [S18]

Telemetry	Investigation hypothesis	Caution
Sophos managed detections	Check deployed IPS 213184, 213185, 213187, 213188 and 213189 and iSensor 62983, 62986, 62988 where applicable.	Rule availability is product-specific. A rule alert describes a detected pattern, not necessarily a successful exploit. [S17]
CISA KEV and external threat reporting	Both CVEs appear as known exploited on 26 Oct; investigate prioritised assets and record forensic triage decisions.	This is threat context and a federal directive indicator, not per-host forensic proof. Due date is not universally applicable. [S24]
Research honeypot RCE	Look for Apache/mod_php parent-child shell activity with multipart requests, PHP OOM, memory leaks, early HTTP 200 and subsequent worker aborts.	35 honeypot shell starts on 24 Oct were correlated to research sensors, not customer environments. [S26]
PAN-OS management attack targeting	Review exposed management HTTPS/XML API, approved jump-host sources, unusual API or admin activity and vendor threat content coverage.	Palo Alto now reports active exploitation targeting interfaces; local successful compromise still needs corroboration. [S25]

Expanded compromise investigation: PAN-OS attack chain

Unit 42 independently verified Dream Research tooling/results for a campaign reported to have rooted 24 internet-facing PAN-OS firewalls and one internal management server. The recovered chain used PHP2Shell plus a separate Linux kernel privilege escalation (CVE-2026-46300). The latter is a distinct vulnerability, not a new PHP fixed version. Look for evidence appropriate to exposed devices, not an assumption of compromise. [S35-S37]

Preserve logs/config and investigate suspicious requests to management interfaces, unexpectedly spawned shells or PHP webshells, root-level persistence, anomalous outbound SSH/SOCKS tunnels, service restarts/crashes, new or modified PHP files including the reported /unauth/php/change_password.php, and persistence scripts or startup hooks under /usr/local/lib/.panops/. Treat published paths as case-specific indicators that may not appear in other attacks. [S36]

If compromise is supported, assess extracted device secrets, LDAP service account material, HA/certificate/private keys, identity-provider integrations, unexpected domain enumeration, password-spraying attempts, unauthorized AD account creation and SAML signing key access. Dream reports credential extraction and directory enumeration but could not confirm success of password spraying, backdoor account creation or SAML key extraction. Preserve this distinction. [S36]

Lookback: retain the existing 17 October minimum based on observed attempts; Sophos 28 October guidance recommends investigating exposed systems back to 1 August 2026 where logs and business context allow, due to the earlier private-report timeline. Label earlier review as precautionary, not proof attacks occurred on 1 August. [S41]

Response after credible privileged execution or persistence

For positive evidence on a PAN-OS or other embedded device, escalate to the vendor and qualified incident response; preserve volatile/nonvolatile evidence before disruptive operations where feasible. Patch or rebuild from trusted media and verify removal of webshells/tunnels. Rotate impacted service-account, admin, VPN, API, certificate or signing credentials based on evidence and risk. Review trusted inter-device relationships and audit downstream identity systems. Coordinate legal/insurer reporting if applicable. [S35-S37]

CASMA/F5/Siemens hunt extension: preserve available administrative access logs, web request logs, process and outbound connection telemetry for historically exposed services, subject to vendor-supported methods and customer authorization. Investigate abnormal process creation, service configuration changes and outbound tunnels only where evidence supports those observations. No CASMA-, F5- or Siemens-specific successful compromise is established by the reviewed 3 November national alert; do not invent IOCs or infer execution from a blocked WAF request. [S51-S55]

7 NOV HUNTING SCOPE EXTENSION

For Hillstone/FortiSOAR and comparable management appliances, review exposed management paths, authentication/configuration activity, web/service crashes, unexpected process creation and egress within available vendor telemetry. For Cloudflare events correlate rule ID/action, edge request, origin outcome and asset logs. Record "blocked attempt", "suspected exploit", "confirmed execution" and "customer compromise" separately; only the latter two require appropriate affirmative evidence. [S58, S62-S64]

7.3 Escalation trigger

Escalate promptly when available evidence suggests web-worker code execution, persistence, credential or data access, or credible unexplained post-exploit behavior. Open an IR case and preserve process, disk and log evidence under the organization’s evidence-handling policy. Contain first in coordination with the customer. Then scope lateral movement, secrets and databases, determine legal/insurance notification requirements with counsel, and rebuild from trusted sources when integrity cannot be demonstrated.

8. Communicate with customers and third parties

8.1 Required communication cadence

Send an initial notice to affected or potentially affected customers with what is known, what is under assessment, which business decisions may be needed, who owns third-party providers, and the next update time. Use a different message when exposure is verified absent versus still unknown.

8.2 Initial customer advisory - adaptable text

We are assessing PHP2Shell (CVE-2026-109618 and CVE-2026-109619) across assets and vendor services in our agreed management scope. CISA added both vulnerabilities to its Known Exploited Vulnerabilities catalog on 26 October 2026; this increases investigative urgency but is not evidence that your environment was compromised. We are prioritizing exposed PHP-serving and embedded management interfaces, verifying vendor-specific patches and reviewing retained activity back to at least 17 October where available. Your environment-specific exposure, patch and compromise-review status will be provided by [UTC date/time], with any open decisions assigned to an owner. [S24-S25]

Suggested customer clarification after 29 October

Our review separates three questions: was the service exposed and vulnerable; was it corrected and verified; and does retained evidence support attempted or successful exploitation, persistence or downstream identity compromise? Industry research has validated successful attacks against some PAN-OS devices, but that does not establish compromise of this customer. We will disclose confirmed findings, evidence gaps and next actions by [UTC date/time]. [S35-S38]

8.3 Third-party provider request - adaptable text

Please confirm whether [service/product/build] embeds affected PHP or an affected management/Edge Computing component; identify the exact product, interface, external reachability, impacted CVE(s), fixed vendor build for BOTH PHP2Shell CVEs, whether that build is available now (not only planned), installation/activation time and independent proof. For PAN-OS provide branch-specific hotfix and management access controls; for Tenable provide SC-202610.2; for Peplink give ICVA or Balance/MAX model, hardware revision and firmware; for Cisco provide bug/build and prerequisites. Describe logs from 17 October onward where retained, distinguish blocked attempts from actual shell/code execution and identify any inability to complete forensic triage. Return official advisory URL, responsible owner and next update UTC. Address separate CVE-2026-115560 and Brotli CVE-2026-111497 only where product applicability is verified. [S21, S24-S30]

Additional third-party verification questions

Request the exact installed fixed package/build and evidence for each dependent product (PAN-OS/Panorama, NetScaler, Synology PHP and apps, Citrix/Check Point/Cisco/Carbon Black, Azure and legacy TuxCare), historic management exposure, WAF effective configuration, service restart, vendor-specific compromise indicators and credential/access-impact assessment. Where an image/firmware fix is not yet installed, require a named owner, interim isolation and a time-bounded exception. [S35-S49]

For Broadcom CASMA, please supply product advisory 39475 or an official support case response stating affected builds, fixed version, deployment date, current running build and incident evidence. State clearly if the installation is Content Analysis (CAS) rather than CASMA. For F5 BIG-IP, identify Configuration utility and APM exposure plus the installed fixed branch/hotfix. For Siemens RUGGEDCOM APE1808, confirm the exact PAN-OS version, applicable Siemens-approved update and management exposure. Provide separate responses for remediation and compromise review. [S51-S54]

7 NOV PROVIDER ATTESTATION QUESTIONS

Ask: Which exact PHP package/image/firmware is running? Does its vendor changelog cover both CVEs? Who maintains the runtime? Is the service hosted or customer-managed? Are WAF and management-interface restrictions configured on the actual request path? For cPanel/TuxCare ELS, did packages survive nightly maintenance after CPANEL-58351? For FortiSOAR/Oracle, provide the current product-specific affected/fixed matrix rather than a general marketing assurance. [S57-S65]

8.4 Closure notice - adaptable text

Assessment for [customer/scope] is complete as of [UTC date/time]. We evaluated [count] in-scope assets and [count] third-party dependencies. [Count] vulnerable installations were verified remediated, [count] have approved exceptions and [count] remain under vendor investigation. We performed the compromise review described in [report reference]; no assessment can guarantee that no historic exploitation occurred. Outstanding actions, owners and dates appear in the attached register.

Customer communication must avoid statements like “fully safe,” “not exploited” or “all systems protected” without corresponding evidence and an expressly defined scope. Clearly identify third-party assertions that the MSP has not independently confirmed.

9. Track, report and close

9.1 Exclusive working status values

Status	Meaning
NOT EVALUATED	Asset or customer scope identified but evidence review not started.
UNKNOWN	Assessment attempted; insufficient evidence, missing permissions or missing provider confirmation.
NOT AFFECTED - VERIFIED	The defined scope has adequate evidence of no affected PHP use or no relevant exposure; a patched formerly vulnerable runtime belongs under PATCHED - VERIFIED.
VULNERABLE	Unpatched affected serving runtime confirmed.
TEMPORARILY MITIGATED	Interim control applied; complete patch still required.
PATCHED - UNVERIFIED	Change reported or installed; serving runtime and validation pending.
PATCHED - VERIFIED	Correct fix active in serving runtime, workers replaced and tests passed.
SUSPECTED COMPROMISE	IR investigation opened; do not hide behind patch status.
EXCEPTION APPROVED	Named customer risk owner approved retained risk, controls and expiry.

An individual asset can require both a remediation status and a separate compromise-review status. Keep those fields independent. A provider dependency is not “complete” until evidence is adequate or responsibility is formally transferred with customer acknowledgment.

9.2 Daily coordinator report

Report scope by customers and assets, statuses PATCHED - VERIFIED / PATCHED - UNVERIFIED / vendor pending, open exceptions, and unknowns. Include Cisco and PAN-OS/Panorama products when applicable. Provide number and coverage of retrospectives since 17 October, logging gaps, attempted/blocked events and substantiated code execution or compromise as DIFFERENT counts. Record pending CVE-2026-115560 configuration mitigation separately from PHP2Shell patch status. [S17-S23]

9.3 Closure gate

1. Every customer in scope has received an assessment disposition or explicit bounded limitation.
2. Every discovered PHP instance has runtime, owner, serving-path evidence and remediation status, or remains in an assigned open-risk register.
3. Every applicable third-party dependency has vendor response evidence or documented escalation and risk acceptance.
4. Every patch is verified in the active runtime; all affected workers/images are replaced.
5. Each exposed asset has an explicit retrospective-review disposition covering at least 17 October 2026 when logs exist. The review records unavailable intervals, IOC matches and category of evidence (scan,

failed/blocked attempt, laboratory-only claim, confirmed asset execution, confirmed follow-on compromise). Do not equate a WAF block with compromise, a patch receipt with clean history, or missing alerts with assurance. Escalate credible signs under the IR process. [S12, S17-S18]

6. Final customer notice and internal after-action review are recorded. Recheck later vendor advisories and missed discovery leads.

7. Affected Cisco and other embedded-vendor products have build/patch-availability evidence or a named open-risk owner with a dated recheck. Document Cisco bug-specific workarounds and access prerequisites rather than assuming upstream PHP packages patch an appliance. [S21]

8. For PHP session upload progress, document ongoing temporary control or unaffected configuration while awaiting the separate CVE-2026-115560 regular-cycle fix; do not report this as closed merely because PHP2Shell patches are installed. [S23]

9. Record CISA KEV status for BOTH CVEs, whether the customer is subject to any federal due-date/forensic-triage rules, and the separate factual determination of compromise. Record Palo Alto management-plane exposure and observed attack telemetry, and vendor-issued hotfix availability versus installed/verified status. Do not close Peplink or Tenable dependencies based on an upstream PHP version alone. [S24-S29]

Additional closure gates for this consolidated edition

Do not close an exposed PAN-OS incident solely on hotfix installation. Require a documented separate compromise/persistence review and disposition of privileged or identity-system access if evidence justifies investigation. If evidence is incomplete, preserve a bounded UNKNOWN/open-IR status with next review date. [S35-S37]

For Synology, close only once the specific Calendar, Mail Station (manual update), and PHP packages are verified or the affected service is isolated/retired. For Azure, separate provider-managed platform updates from customer-owned runtime/image updates. For Citrix and WAF products, a generic WAF rule is not proof of management-plane remediation. [S39-S47]

3 NOVEMBER VENDOR-SPECIFIC CLOSURE: Do not close an affected CASMA item from the Broadcom umbrella advisory alone; require a support-backed product version disposition or maintain an explicitly owned open risk. For BIG-IP, verify fixed TMOS branch/hotfix plus both APM data-plane and Configuration utility control-plane exposure. For APE1808, verify approved patched PAN-OS installation and restricted management paths. Record separately any historic exposure, suspicious activity and response findings. [S51-S55]

7 NOV CLOSURE REQUIREMENTS

Do not close on version banner, scan-cleared finding, patch publication, WAF block or deployment success alone. Save signed/dated verification of active patched PHP or vendor firmware, approved and completed change, after-restart functional checks, unresolved exceptions, and separate investigation outcome. Repeat post-maintenance verification for cPanel ELS or rebuilt containers where drift is plausible. [S59-S62]

10. Runbook for exceptions, failures and disagreements

Provider will not confirm patch status

Record UNKNOWN, request vendor package and timestamp, escalate through customer owner, and consider compensating access restrictions or migration. Do not mark “not affected” based on silence.

Application breaks after patch

Invoke the approved rollback and outage process; preserve logs; document service restoration; isolate the vulnerable service if rolled back. Do not silently leave it exposed after restoring service.

Conflicting version results

Reconcile CLI PHP, front-end handler, active worker executable/module, multiple FPM pools, container tags/digests and control-panel-selected version. Record each rather than choosing the newest result.

Possible compromise discovered during change

Pause destructive remediation long enough for the incident-response lead to preserve relevant evidence. Make containment and customer notification decisions under the IR process, then patch or rebuild under directed response.

Customer refuses downtime

Present patch, restricted-access, temporary suspension and formally accepted risk options. Record who accepted residual risk and when it expires. Never equate a business exception with a fixed system.

Appendix A. One-page technician field checklist

Discover

- [ ] Customer and asset ID
- [ ] Application owner and business function
- [ ] All runtime paths and versions
- [ ] Serving SAPI/worker/image
- [ ] Exposure: internet / internal / localhost / CLI
- [ ] Vendor or hosting dependencies

Remediate

- [ ] Fixed upstream or documented backported package
- [ ] Change approval and rollback plan
- [ ] If IR concern, preserve evidence first
- [ ] Update all instances and replace workers
- [ ] Validate functionality and access controls

Verify and close

- [ ] Serving-runtime proof
- [ ] Security telemetry and compromise disposition
- [ ] UTC timestamp and reviewer
- [ ] Customer notice
- [ ] Open vendor items/exceptions with owner and date

Appendix B. Platform verification quick reference

Platform	Inventory / validation emphasis	Evidence to keep
Windows / IIS	IIS FastCGI mapping and php-cgi path, TS/NTS compatibility, old process exit, extensions.	Mapping screenshot or config, binary version, worker restart and smoke tests.
Apache mod_php	Loaded libphp module, package build and httpd graceful/full restart outcome.	mod_php package evidence, active workers and application checks.
Nginx / FPM	Per-site fastcgi_pass, pool socket/service, pool package and active worker lifetime.	Pool map, PHP-FPM package, restart, route tests.
cPanel / CloudLinux	Panel build, EA-PHP/ALT-PHP package releases, domain-selected handlers.	Vendor release matrix and package transaction log.
Plesk	Plesk-shipped PHP handlers and additional Plesk components.	Current Plesk advisory, package identifiers, restart proof.
Containers / Kubernetes	Image base, registry digest, rebuild pipeline and ALL running replicas.	New digest, rollout status, in-container runtime, app tests.
Managed website / SaaS	Provider patch statement tied to exact service/tenant and date.	Vendor response, corroborating checks, exception if uncertain.
PAN-OS / Panorama	Management web UI and XML API accessibility, exact vendor branch, jump-host-only restriction; distinguish GlobalProtect portal.	Palo Alto advisory/current fixed-build ETA, ACL review, owner, scope and exposure proof. [S13]
CloudLinux package families	Differentiate ea-php, alt-php and native; do not rely only on php -v or --security update filtering.	Vendor-specific backport changelog or rebased upstream version; statuspage snapshot and active workers. [S11]
Cisco Expressway / Select	Verify bug CSCwx37062; release target 15.5.21 (TBD); Cisco-documented bug-specific workaround.	Current exact appliance build, bug notice, control applied, owner, patch check date. [S21]
Cisco URWB	Verify bug CSCwx37073; release target 27.1.1 (est Feb 2027); administrator-authentication prerequisite; bug-specific workaround.	Administrative access exposure, workaround, customer approval, patch availability follow-up. [S21]
Cisco Duo Access Gateway	Verify fixed release 3.2.0 and check whether customer deployed it.	Device/software build, vendor release record, test and owner. [S21]
CloudLinux ELS ALT PHP repository	Confirm php-els is enabled if previously added; status update 23 Oct 21:36 UTC supersedes old disable guidance.	Repo state, cloudlinux-release version, cPanel cl-ea4 state, version/changelog. [S19]
PAN-OS / Panorama: 27 Oct	Exposed management HTTPS/XML API (including management-profiled dataplane), exact branch/hotfix. Advisory lists released and future ETA builds; GlobalProtect is NOT affected.	Official Palo Alto fix matrix timestamp, installed/active build, access ACL, threat-inspection prerequisites, separate Brotli note for 11.2.10-h16. [S25]

Platform	Inventory / validation emphasis	Evidence to keep
Tenable Security Center / Enclave Security	Confirm whether Security Center <=6.9.1 / Enclave <=1.9.1; obtain product patch SC-202610.2 for the specific supported release.	Vendor patch installation record, application build, restart and product-level verification. [S27-S28]
Peplink ICVA	ICVA <=2.14.3 affected; update to 2.14.4. Restrict TCP 4443 to trusted networks until patched.	Exact ICVA firmware, management reachability, update and reboot verification. [S29]
Peplink Balance / MAX with Edge Computing	Affected on 8.6.1 GA when Edge Computing enabled. Use 8.6.1s042 only for listed model and hardware revision; disable/isolate ContentHub in interim.	Model/HW rev and EC state, vendor firmware link, effective restrictions and active firmware. [S29]
Windows PHP binaries -1 rebuild	Official 8.2.35-1 / 8.3.36-1 / 8.4.27-1 / 8.5.12-1 Windows builds fix distinct bundled Brotli issue. PHP2Shell source versions unchanged.	Package hash/SBOM when available, loaded TS/NTS build and PHP worker replacement. [S30]

PLATFORM VERIFICATION NOTES | 27 OCT BASELINE + 28-31 OCT ADDITIONS

cPanel: verify panel version separately from EasyApache4; published patched panel builds include 110.0.153, 134.0.66, 136.0.50 and 138.0.18. EasyApache4 fixes include ea-php74 7.4.33-19, ea-php80 8.0.30-12 and ea-php81 8.1.34-5; verify affected installation against the live cPanel matrix. A package changelog search such as rpm -q --changelog ea-php81-php-cli | grep -m1 CVE-2026-109618 is one vendor-documented verification method. [S4]

Plesk: its Linux PHP 7.4/8.0/8.1 patched backports may report the same version number but show a build date of 21 Oct 2026. Plesk Obsidian management fixes are 18.0.80 Update 11 or 18.0.81 Update 4 for sw-engine/plesk-engine. Windows packages for PHP 8.2-8.5 have fixed upstream versions. Verify current applicability and availability. [S5]

CloudLinux: the 23 October status confirms fixed native PHP in stable for every affected CloudLinux stream and upstream-numbered alt-php and ea-php 8.2-8.5 packages in stable; older backported builds already addressing BOTH CVEs remain fixed. Verify exact distro/family and the running PHP handler, not an upstream number alone. A security-only package filter can miss EA4/ALT advisory metadata. Check cloudlinux-release and cl-ea4 if updates seem absent. UPDATE 23 OCT 21:36 UTC: KEEP the ELS ALT PHP (php-els) repository enabled if it was added; the status page corrects earlier disable advice. [S11, S19]

Palo Alto Networks, consolidated through 29 Oct: the earlier v1.2 statement of no known malicious exploitation is superseded by Unit 42 independent verification of Dream Research attacker tooling and successful campaign results. The vendor confirms active exploitation targeting internet-facing PAN-OS/Panorama management interfaces. Branch-specific fixed hotfixes are documented across supported PAN-OS 10.2, 11.1, 11.2, 12.1 and 12.2; 11.2.10-h16 does NOT resolve the separate Brotli issue, whereas h17 does. Any customer-specific compromise conclusion still requires local evidence. [S35-S38]

Cloudflare/Imunify360: confirm active protection at the edge and no alternate origin exposure. Cloudflare reports request-plus-response transaction-based detection; Imunify360 rules cover known upload-progress attack shapes but do not cover every possible exploit path. Record WAF coverage as TEMPORARILY MITIGATED, never as patched. [S6, S11]

PHP separate advisory (23 Oct): PHP requests session.upload_progress.enabled=0 until the next regular fix for CVE-2026-115560 if applicable. This requires an unusual mix of php_binary/php_serialize configuration followed by a runtime switch to php before session_start(); the two original PHP2Shell CVEs are a separate patch requirement. [S23]

Sophos/Arctic Wolf (22-23 Oct): treat Potassium-associated network indicators as hunting leads, not proven infection on a customer host. Sophos corrected a successful-exploitation claim to failed/blocked attempts. Confirm Sophos firewall/endpoint rule deployment, including IDs 213184, 213185, 213187, 213188 and 213189, and investigate PHP worker child-process/downloader activity. [S17-S18]

Cisco (prior 23 Oct baseline, SUPERSEDED by Cisco v1.10 dated 30 Oct): Expressway and Expressway Select Series 15.5.21 now listed as fixed; Duo Access Gateway 3.2.0. ISE Portal Builder fix deployed, no customer action required. For URWB and Unified Industrial Wireless Software, check the Cisco product/bug matrix: as of 30 Oct Cisco lists 26.2.1.9 as a planned Nov 2026 fix for the applicable wireless product, with privileged-administrator exploitation prerequisite. Do not use the old February 2027 ETA as current. Verify vendor applicability and release availability. [S42]

Tenable (23 Oct): Security Center 6.9.1 and earlier and Enclave Security 1.9.1 and earlier require review. Tenable issued SC-202610.2 to update bundled PHP to 8.2.35; confirm exact product/release and installation. Peplink (23 Oct): ICVA <=2.14.3 is affected; ICVA 2.14.4 is the fixed firmware. Balance/MAX routers with Edge Computing enabled on firmware 8.6.1 GA require model/HW-specific 8.6.1s042. Vendor-hosted InControl 2 is unaffected. Verify interface restrictions until patched. [S27-S29]

Honeypot/KEV status (26-27 Oct): SecurityWeek documents 35 correlated shell starts across three controlled mod_php honeypots on 24 Oct, evidence consistent with CVE-2026-109618. CISA KEV entries dated 26 Oct apply to BOTH CVEs and flag forensic triage. The 29 Oct KEV date is federal, not a universal private-sector deadline. CISA publication does not expose the underlying evidence or name customer victims. [S24, S26]

1 NOVEMBER CONSOLIDATED VENDOR QUICK REFERENCE

The rows below are snapshots of manufacturer guidance reviewed for this edition. Recheck the linked live advisory before applying any specific build and document the installed build and actual exposure. Unsupported releases require special handling. [S38-S49]

Product / scope	Fixed release or action	Verification / limitation
PAN-OS / Panorama	12.2.4-h1; 12.1.4-h13 / 12.1.7-h11 / 12.1.10-h3	Other PAN-OS branches below; exact maintenance branch must match Palo Alto advisory.
PAN-OS 11.2	11.2.4-h23 / 11.2.7-h23 / 11.2.10-h16 / 11.2.13-h4 / 11.2.16-h1	11.2.10-h16 covers PHP2Shell, not separate Brotli; 11.2.10-h17 covers both.
PAN-OS 11.1	11.1.4-h38 / 11.1.6-h40 / 11.1.7-h12 / 11.1.10-h36 / 11.1.13-h16 / 11.1.16-h4	Check exact target/hotfix and management reachability.
PAN-OS 10.2	10.2.7-h39 / 10.2.10-h42 / 10.2.13-h27 / 10.2.16-h12 / 10.2.18-h13	Older unsupported versions: move to supported fixed release.
NetScaler ADC / Gateway	14.1-73.49+ or 13.1-64.32+	Management NSIP, management-enabled SNIP and cluster IP; backend WAF != management fix.
NetScaler FIPS / NDcPP	14.1-FIPS 14.1-73.49+; 13.1-FIPS/NDcPP 13.1.37.286+	Select correct certified branch.
Cisco Expressway / Select	15.5.21	Latest Cisco PSIRT confirms fixed build.
Cisco Duo Access Gateway / ISE Portal Builder	Duo 3.2.0; ISE Portal Builder fixed by vendor	For ISE Portal Builder, Cisco reports no customer action.
Check Point web interfaces	Vendor product hotfix sk1000302; Spark fixed R81.10.17 / R82.00.11	Require portal use, exact hotfix/revision and official support portal evidence.
Carbon Black App Control Server	8.12.2 or 8.13.2	Vendor advisory and installed server build.

Product / scope	Fixed release or action	Verification / limitation
TuxCare ELS native / alt-php	Full repo-specific vendor release / backport	ELS for OS and separate ELS for PHP are different subscriptions.
Azure managed/customer PHP	Built-ins updated where supported; customer custom PHP/image patch required	Check service, platform channel, container digest and worker.
Synology DSM PHP and apps	See DSM matrix below	Built-in DSM PHP is not externally exposed; apps need separate verification.
Broadcom CASMA vs CAS	CASMA: AFFECTED; fixed build not established in public ESG umbrella advisory. CAS: NOT VULNERABLE.	Verify full product name and obtain Broadcom CASMA notice 39475 or vendor support answer; no invented version. [S51-S52]
F5 BIG-IP APM and Configuration utility	F5 K000163821: fixed 17.1.3.7 / 17.5.1.11 / 21.1.0.4 (as applicable); vendor ENG hotfix alternatives.	APM data-plane access profile vs all-modules Configuration utility control plane; separate backend WAF rules. [S53]
Siemens RUGGEDCOM APE1808 + PAN-OS	Affected PAN-OS 10.2 / 11.1 / 11.2 / 12.1 / 12.2: use corresponding available fixed PAN-OS update.	Siemens SSA-566512: confirm customer hardware, PAN-OS branch and vendor support/approved upgrade. [S54]

SYNLOGY FIXED PACKAGE REFERENCE (Synology-SA-26:14 revised 31 October 2026)

Package	DSM branch	Minimum fixed package
Calendar	7.2+	3.0.4-21435
Calendar	7.0-7.1	2.4.8-10948
Calendar	6.2	2.4.8-0948
Mail Station (manual)	7.2+	30000002.3.19-20333
Mail Station (manual)	7.0-7.1	30000002.3.19-10333
Mail Station (manual)	6.2	30000002.3.19-0333
PHP 7.4	7.2+ / 7.0-7.1 / 6.2	7.4.33-0131 / -0122 / -0010
PHP 8.0	7.2+ / 7.0-7.1	8.0.30-0122 / -0104
PHP 8.1	Applicable	8.1.34-0120
PHP 8.2	Applicable	8.2.35-0171
PHP 8.3	Applicable	8.3.36-0051
PHP 8.4	Applicable	8.4.27-0051
PHP 7.3	All	No Synology fix; migrate, disable or retire affected application.

Note: a source package fixed on one DSM branch is not evidence the same build is fixed on another branch. DSM earlier than 6.2 requires special isolation and migration guidance. Synology Drive and Hyper Backup are listed not affected. [S46-S47]

7 NOV PLATFORM ADDENDUM

Snipe-IT official images: Ubuntu v8.8.2; Alpine v8.8.3-alpine. Record deployed digest and PHP runtime. EGroupware official patched images: 26.10.20261021 and 23.1.20261021; hosted rollout is a separate vendor assertion. Centreon Cloud: patched-hosted claim; on-premises requires distributor patch validation. [S57, S60]

Qualys Windows/macOS: identify unmanaged runtimes; upgrade within supported minor series using authorized processes; Homebrew scope on macOS; EOL versions demand supported backports or migration.

cPanel: CPANEL-58351 on documented 110.0.155 / 134.0.68 / 138.0.21; check TuxCare ELS package persistence. [S59, S61]

Hillstone: IPS 6.4.1; BDS 6.4.1; NGFW 5.5R12P4.5 (specific branch). CloudHive/LMS and ADC not to be marked fixed pending vendor schedule. FortiSOAR/PaaS: national CSIRT lists affected products; obtain exact fixed version from current Fortinet PSIRT. Oracle: follow product-specific alert entries. [S62-S65]

Appendix C. Master tracker, vendor tracker and decision log

The companion toolkit provides three CSV templates suitable for an RMM export, PSA ticket view or managed workbook. Use a controlled repository and define retention and access rules before putting customer data in it. No customer data is included in the templates.

- Customer-Asset-Tracker.csv: asset identity, scope, serving PHP, version, SAPI, evidence, risk, owner, change, verification and compromise review.
- Vendor-Dependency-Tracker.csv: product, provider contact, advisory, package/fix confirmation, escalation and follow-up.
- Response-Decision-Log.csv: timestamps, options, authorization, residual risk, customer approval and review date.

Appendix D. Advisory monitoring and document maintenance

Monitor PHP, both GHSAs, CISA KEV, NCSC-NL software inventory and vendor advisories daily while the emergency remains active. Preserve dated snapshots because vendor statements can change materially: Sophos corrected success claims; Palo Alto later changed from no known exploitation to active targeting; CloudLinux revised ELS repository instructions. Record exact source version, UTC checked, current hotfix availability, applicable forensic triage, evidence confidence, outstanding customer approvals and next check. Never silently revise a distributed download while retaining the same version label. [S17, S19, S24-S31]

Trigger	Required playbook review
New fixed/backported package	Update affected-branch table and platform appendix; add provider evidence requirements.
Confirmed new exploit path or new SAPI impact	Reassess P0/P1, hunt coverage and interim restrictions.
Observed active exploitation or new IOC	Update hunt checklist, investigation window and customer notification language.
Mitigation withdrawn or WAF rule changed	Recheck compensating control, exception register and patch urgency.
New vendor product identified	Expand discovery universe and third-party dependency requests.
New pre-disclosure attempt telemetry	Extend retrospective hunt to at least 17 Oct 2026 for exposed systems; label unknown logs and distinguish attempts from compromise. [S12]
Source correction or new related CVE	Replace withdrawn claims; update evidence labels. Keep adjacent CVEs and their mitigation/patch status separate. [S17, S23]
CISA KEV listing / changed vendor exploitation statement	Update incident priority, forensic triage gate, customer notices and evidence confidence; distinguish active targeting and honeypot success from customer compromise. [S24-S26]

Trigger	Required playbook review
Vendor hotfix changes ETA to released	Verify the exact branch/build in official downloads, update exposure register and test the installed active version. Recheck other still-pending branches. [S25]

1 NOVEMBER REVISION CONTROL AND MONITORING

When a vendor advisory changes, record advisory timestamp, exact changed fixed-build claims, what was already known, what is now newly available, customer applicability and an independently verified installation record. Examples of material status revisions in this edition: Palo Alto released the remaining branch hotfixes; Cisco v1.10 superseded older fixed-release estimates; Synology expanded DSM 6.2/7.0/7.1 Calendar and Mail Station package coverage; Cloudflare revised detection rules on 30 October. [S38,S42-S43,S46]

Distinguish CISA KEV determination; attacker telemetry; vendor-confirmed production exploitation; blocked attempts; local device execution; and specific named customer incidents. Do not infer successful compromise from WAF logs or infer no compromise from clean scans. Record confidence, retention gaps, and 17 October minimum / optional 1 August retrospective start separately. [S35-S37,S41]

3 NOVEMBER SOURCE MONITORING: Broadcom CASMA vs CAS status changed 30 October, NCSC-NL cataloged the distinction on 2 November, and CSA issued a national multi-vendor alert on 3 November. For CASMA, treat public fixed-build detail as unknown pending access-controlled notice 39475. F5 K000163821 and Siemens SSA-566512 provide distinct product/feature scopes. Do not re-label known PAN-OS production compromises as newly confirmed CASMA, F5 or Siemens incidents. Save vendor advisory revisions and actual customer version evidence. [S51-S56]

7 NOVEMBER 2026 MONITORING SNAPSHOT

Recheck official PHP/GHSA, NCSC-NL repository and the manufacturer pages before changing a customer status. Software inventory snapshot dated 4 Nov contains 948 tracked entries; it is an evolving index and not a substitute for product fixed-release evidence. Date a future advisory update by the date the underlying product status actually changed, not merely the day an inventory row was cataloged. [S1-S3, S57]

Sources and source-status register

Version 1.5 is a focused maintenance release dated 3 November 2026, preserving the 1 November consolidated v1.4 response architecture. It adds Broadcom CASMA/CAS disambiguation, F5 BIG-IP APM vs Configuration utility scope, Siemens RUGGEDCOM APE1808 running PAN-OS, and a dated NCSC-NL classification snapshot. CISA KEV includes both PHP2Shell CVEs and confirmed PAN-OS campaign exploitation remains relevant, but evidence of that campaign does not prove compromise of other named products. Revalidate each vendor build and customer installation before declaring remediation. Upstream PHP2Shell fixed source versions remain 8.2.35, 8.3.36, 8.4.27 and 8.5.12. [S1-S3,S51-S56]

[S1] PHP Security Team, Critical remote code execution vulnerabilities, 21 Oct 2026. Source page

[S2] PHP / php-src GHSA-w8hw-w9fx-j79w, RCE via OOM corruption. Source page

[S3] PHP / php-src GHSA-6wmf-4rv5-p3rp, RCE via stale global state. Source page

[S4] cPanel, Critical PHP Security Release. Source page

[S5] Plesk, Remote code execution in PHP shipped with Plesk. Source page

[S6] Cloudflare, Deploys protections against php2shell, 21 Oct 2026. Source page

[S7] Netherlands NCSC, PHP2Shell operational repository (public). Source page

[S8] Armis, PHP2Shell: How to Find, Prioritize, and Patch Affected Systems. Source page

[S9] CERT-EU, Security Advisory 2026-018. Source page

[S10] PHP Supported Versions. Source page

[S11] CloudLinux, PHP CVEs and Imunify360 interim rule guidance. Source page

[S12] Amazon Threat Intelligence, MadPot PHP2Shell attempted exploitation starting 17 Oct; published 21 Oct 2026. Source page

[S13] Palo Alto Networks, PHP2Shell impact across PAN-OS and Panorama; initial advisory 21 Oct 2026. Source page

[S14] CloudLinux, live PHP2Shell package status and availability updates, 22 Oct 2026. Source page

[S15] Plesk, version/build-specific fixed runtimes and management engine; updated 22 Oct 2026. Source page

[S16] cPanel, updated panel and EasyApache4 patch matrix; updated 22 Oct 2026. Source page

[S17] Sophos X-Ops: Proof-of-concept exploit released for PHP vulnerabilities; corrected Oct 22 21:21 UTC; updated Oct 23 19:31 UTC. Source page

[S18] Arctic Wolf Labs: PHP2Shell attempted payload retrieval and Potassium infrastructure, Oct 22. Source page

[S19] CloudLinux: PHP2Shell live incident/status including 23 Oct 13:10 UTC ea-php update and 21:36 UTC php-els correction; CloudLinux verification KB updated Oct 23. Source page

[S20] VulnCheck: PHP2Shell independent lab RCE results, expanded Oct 23 17:30 ET. Source page

[S21] Cisco PSIRT: Vulnerabilities in PHP Affecting Cisco Products; version 1.6 updated 23 Oct 22:39 GMT. Source page

[S22] CloudLinux: exact alt-php/ea-php patched package guide, updated Oct 23. Read with later status corrections. Source page

[S23] PHP project: Informational advisory, Session upload progress, Oct 23; separate CVE-2026-115560. Source page

[S24] CISA KEV data mirror, official CISA repository; both CVEs dateAdded 26 Oct 2026, forensicTriage=Yes, dueDate=29 Oct 2026. Source page

[S25] Palo Alto Networks CVE-2026-109618 advisory, updated 27 Oct 2026; active targeting statement, severity, released/pending hotfixes, caveats. Source page

[S26] SecurityWeek, 26 Oct 2026; reports forensic evidence from 24 Oct research honeypots and 35 confirmed shell executions. Source page

[S27] Tenable Security Center product advisory TNS-2026-30, 23 Oct 2026; SC-202610.2. Source page

[S28] Tenable Enclave Security product advisory TNS-2026-31, 23 Oct 2026; SC-202610.2. Source page

[S29] Peplink official PHP2Shell advisory, 23 Oct 2026; ICVA/Edge Computing impacts, firmware and mitigations. Source page

[S30] PHP 2026 security notices, 26 Oct Windows -1 Brotli rebuild and 21 Oct PHP2Shell source releases; see dated release records. Source page

[S31] NCSC-NL PHP2Shell operational repository and updated software inventory, 27 Oct 2026. Source page

[S32] Cloudflare protective WAF guidance, 21 Oct with 23 Oct update; limits of detection and session feature control. Source page

[S33] PHP source GHSA-109618, ongoing authoritative impact/mitigation guidance. Source page

[S34] PHP source GHSA-109619, ongoing authoritative impact/mitigation guidance. Source page

[S35] 29 Oct 2026: Palo Alto Unit 42, independently verified attacker tooling and PAN-OS exploitation. https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/

[S36] 26 Oct, revised 29 Oct 2026: Dream Research, chained PHP2Shell + kernel LPE; case-specific exploitation artifacts. https://dreamgroup.com/blog/chained-php2shell-exploit-roots-25-servers

[S37] 28 Oct 2026: CISA KEV, distinct Linux kernel CVE-2026-46300 (use live federal KEV data). https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2026-46300

[S38] updated 29 Oct 2026: Palo Alto PAN-OS and Panorama affected versions, full fixed-build matrix and Brotli caveat. https://security.paloaltonetworks.com/CVE-2026-109618

[S39] 27 Oct 2026: Citrix CTX697263, NetScaler ADC/Gateway and FIPS/NDcPP fixed builds. https://support.citrix.com/external/article/CTX697263/citrix-security-advisory-for-cve20261096.html

[S40] Oct 2026: Citrix management-interface restriction and backend WAF distinction. https://community.citrix.com/techzone-blogs/110_security-updates/protecting-netscaler-management-access-from-php-cve-2026-109618-cve-2026-109619-r1640/

[S41] 28 Oct 2026: Sophos Firewall v22/v23 WAF hotfix; optional earlier forensic lookback. https://www.sophos.com/en-us/security-advisories/sophos-sa-20261021-php2shell

[S42] updated 30 Oct 2026: Cisco PSIRT v1.10, updated fixed release availability and prerequisites. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-Jj384Daq

[S43] 30 Oct 2026: Cloudflare WAF changes to PHP2Shell detection expressions. https://developers.cloudflare.com/changelog/post/2026-10-30-waf-release/

[S44] 30 Oct 2026: TuxCare PHP2Shell alt-php/OS ELS backport availability and subscription distinction. https://support.tuxcare.com/hc/en-us/articles/31402484781596-Critical-PHP-vulnerabilities-CVE-2026-109618-CVE-2026-109619

[S45] 30 Oct 2026: MSRC, Azure and customer-managed Windows/container PHP obligations. https://www.microsoft.com/en-us/msrc/blog/2026/10/patch-now-php2shell-brotli-emudhra-guidance-for-customers

[S46] revised 31 Oct 2026: Synology-SA-26:14 exact Calendar, Mail Station and PHP fixes by DSM branch. https://www.synology.com/en-global/security/advisory/Synology_SA_26_14

[S47] updated 29 Oct 2026: Synology advisory statement, affected package scope and MailStation manual update. https://www.synology.com/en-global/company/news/article/php2shell/Synology%20extends%20PHP2Shell%20security%20updates%20to%20end-of-life%20DSM%20versions

[S48] software inventory updated 30 Oct 2026: NCSC-NL PHP2Shell public inventory, product-specific status leads. https://github.com/NCSC-NL/php2shell

[S49] October 2026: Check Point product hotfixes and Broadcom enterprise-product advisory. https://community.checkpoint.com/t5/WAF/PHP2Shell-Technical-Impact-Emergency-Protection-with-Check-Point/td-p/283962

[S50] updated 30 Oct 2026: Broadcom Enterprise Security PHP2Shell response including Carbon Black. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/39404

[S51] Broadcom ESG Advisory 39404, updated 30 Oct 2026: CASMA moved to Affected, CAS Not Vulnerable. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/39404

[S52] Broadcom CASMA product notice 39475, linked by ESG 39404; support login required in public review, fixed-build details not independently accessible. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39475

[S53] F5 K000163821, updated 27 Oct 2026: BIG-IP APM and Configuration utility scope; 17.1.3.7, 17.5.1.11, 21.1.0.4 branch fixes. https://my.f5.com/manage/s/article/K000163821

[S54] Siemens ProductCERT SSA-566512, published 23 Oct and updated 28 Oct 2026: RUGGEDCOM APE1808 with affected PAN-OS versions. https://cert-portal.siemens.com/productcert/html/ssa-566512.html

[S55] Cyber Security Agency of Singapore, AL-2026-157, published 3 Nov 2026: active PAN-OS exploitation and multivendor product review. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-157/

[S56] NCSC-NL php2shell public repository, software status snapshot dated 2 Nov 2026; 930 tracked products, vendor classification leads. https://github.com/NCSC-NL/php2shell

[S57] NCSC-NL php2shell public repository; software list last updated 4 Nov 2026, 948 tracked (185 fixed, 215 vulnerable); product-specific Snipe-IT/EGroupware/Centreon status entries. https://github.com/NCSC-NL/php2shell

[S58] Cloudflare WAF Release, 3 Nov 2026; changed expressions for Free and Managed PHP RCE #2/#3 rules, action remains Block. https://developers.cloudflare.com/changelog/post/2026-11-03-waf-release/

[S59] Qualys blog, 4 Nov 2026; documented CAR Windows/macOS upgrade scripts, supported deployment and EOL limitations. https://blog.qualys.com/product-tech/2026/11/04/php2shell-windows-macos-car-upgrade-scripts

[S60] NCSC-NL 4 Nov vendor inventory references for Snipe-IT, EGroupware and Centreon, incorporating earlier vendor fixes; verify current vendor-specific releases. https://github.com/NCSC-NL/php2shell/tree/main/software

[S61] cPanel 110.0.155 release, 5 Nov 2026, CPANEL-58351; corresponding 134.0.68 and 138.0.21 changelogs should be checked by branch. https://docs.cpanel.net/changelogs/110-change-log/

[S62] Hillstone PSIRT HSVD-2026-0113, published 2 Nov 2026; released and planned product fixes as currently listed 7 Nov. https://www.hillstonenet.com/blog/security_advisory/hillstone-multiple-products-third-party-php-component-remote-code-execution-vulnerability

[S63] Cyber Security Agency of Singapore AL-2026-157, published 3 Nov, updated product list seen 7 Nov, including FortiSOAR and FortiSOAR PaaS; confirms PAN-OS active exploitation. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-157/

[S64] Fortinet PSIRT FG-IR-26-186; verify live affected-version and fixed-build matrix, not independently reproduced in this release. https://fortiguard.fortinet.com/psirt/FG-IR-26-186

[S65] Oracle PHP2Shell Security Alert, Revision 3 dated 6 Nov 2026; product-specific support and patch verification required. https://www.oracle.com/security-alerts/

[S66] PHP core security advisories, 21 Oct 2026, OOM corruption and stale global state. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

[S67] PHP core security advisory, 21 Oct 2026, stale global state. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp

Version history

v1.0 (21 Oct); v1.1 (22 Oct); v1.2 (23 Oct); v1.3 (27 Oct); v1.4 (1 Nov); v1.5 (3 Nov 2026). This maintenance release adds CASMA/CAS product disambiguation, F5 appliance and Siemens APE1808/PAN-OS verification, plus dated vendor monitoring. Detailed mapping and source URLs: CHANGELOG_v1.5.md. v1.6 (7 Nov 2026) integrates operational vendor updates, ELS persistence check, Windows/macOS workflows, WAF signatures and updated appliance patch inventory. Detailed mapping: CHANGELOG_v1.6.md.