Qualys

ONBOARDING GUIDE

PHP2SHELL FREE SERVICE

Find and Fix PHP2Shell on Your Internet-Facing Assets

A step-by-step guide to discovering, scanning, validating and mitigating PHP2Shell with Qualys, starting from nothing more than your domain names.

CVE-2026-109618 CVE-2026-109619

October 2026

Version 1.2

© 2026 Qualys, Inc. All rights reserved.

WELCOME

About this guide

You signed up to find PHP2Shell (CVE-2026-109618 and CVE-2026-109619) across your internet-facing assets. This guide takes you from your first login to a verified fix. Each step tells you which application to open, what to scan and where your results appear. Follow the steps in order.

15 days	1,000	Cloud	Steps 1–5
Free service, from activation	Assets, maximum	Scans run from the Qualys cloud	No agents, appliances or credentials

Contents

— Your onboarding path — Three answers to start with, and the six steps at a glance — 3

00 Before you start — Log in, find your applications, gather what you need — 4

PHASE 1 · FIND PHP2SHELL (NO INSTALLATION)

01 Discover your internet-facing assets — CSAM with External Attack Surface Management (EASM) — 5

02 Scan your hosts for PHP2Shell — VMDR external scan — 7

03 Scan your web applications — TotalAppSec (or WAS) external scan — 9

04 Validate exploitability — ETM TruConfirm external validation — 11

SEE AND FIX

05 Import the PHP2Shell Fightback dashboard — ETM, VMDR or Unified Dashboard — 13

06 Mitigate or patch, then verify — TruRisk Eliminate — 15

OPTIONAL

P2 Deploy a Cloud Agent for authenticated coverage — 18

P3 Connect the tools you already run — 20

— Reference: QIDs, fixed versions and support — 22

© 2026 Qualys, Inc. All rights reserved.

YOUR ONBOARDING PATH

Start here

Three questions to answer before you begin.

01 WHICH APPLICATION DO I OPEN?

Start in CSAM. Every step names its application.

Open applications from the **Application Picker** in the upper-left corner of the Qualys platform.

02 WHAT DO I SCAN?

Your domains first. Nothing inside your network.

EASM turns your domains into a list of public IP addresses and web applications (Step 1). You scan those hosts in Step 2 and those applications in Step 3, all from the Qualys cloud.

03 WHERE DO MY RESULTS APPEAR?

ETM Findings and the PHP2Shell Fightback dashboard.

Every detection appears in **ETM > Risk Management > Findings**. The Fightback dashboard you import in Step 5 brings them together in one view.

The six steps at a glance

	STEP	APPLICATION	WHAT YOU GET
PHASE 1 · FIND PHP2SHELL, NEEDS ONLY DOMAINS AND PUBLIC IPS			
01	**Discover assets** What do we own on the internet?	CSAM · EASM	Inventory of internet-facing hosts and web apps
02	**Scan hosts** Which hosts run vulnerable PHP?	VMDR	PHP2Shell detections on hosts
03	**Scan web apps** Which applications expose it?	TotalAppSec (or WAS)	PHP2Shell detections on web apps and APIs
04	**Validate** Which are actually exploitable?	ETM · TruConfirm	Proof of which hosts are reachable and exploitable
SEE AND FIX			
05	**Dashboard** Where do I see it all?	ETM	One view of your PHP posture
06	**Mitigate or patch** How do I close it?	TruRisk Eliminate	Mitigation or patch, verified by rescan
OPTIONAL · GO DEEPER ONCE YOUR PERIMETER IS COVERED			
P2	**Cloud Agent** What's on each host?	Cloud Agent	Authenticated, host-level coverage
P3	**Connectors** What do my other tools see?	ETM Connectors	EDR and scanner findings next to Qualys findings

© 2026 Qualys, Inc. All rights reserved.

00 BEFORE YOU START

Log in and find your applications

Your **Registration – Start Now** email contains your login credentials and a one-time link to your Qualys platform. The link works only once, so open it from the email when you are ready to begin.

Log in

01 Open the link in the email and log in. Note your platform URL, for example `qualysguard.qg2.apps.qualys.com`. If you have trouble, see the Login FAQ.

02 On first login, accept the End User License Agreement (EULA). The Qualys home page opens.

03 Open the **Application Picker** in the upper-left corner. Your free service includes the applications used in this guide:

- **CyberSecurity Asset Management (CSAM)**, including External Attack Surface Management (EASM)
- **Vulnerability Management, Detection and Response (VMDR)**
- **TotalAppSec (or WAS)**, the updated version of Web Application Scanning
- **Enterprise TruRisk Management (ETM)**
- **TruRisk Eliminate**

04 Keep the PHP2Shell blog open in a separate browser tab. It contains the QIDs, queries and dashboard download this guide uses.

Have this information ready

INFORMATION	USED IN
Your organization's primary domains	Step 1
IP ranges, ASNs or certificate subjects your organization owns (optional)	Step 1
Public IP addresses or FQDNs of your PHP web servers, if known	Step 2
Your public web application URLs	Step 3

> SAVE TIME
> **Import the dashboard first.** The Fightback dashboard (Step 5) fills in as each scan finishes, so your results have one home from the start. **Already know your PHP servers or application URLs?** Start Steps 2 and 3 with them while EASM discovery runs, then add what discovery finds.

> NOTE
> Steps 1–5 need no Qualys Scanner Appliance, Cloud Agent or server credentials. Mitigating through the scanner in Step 6 needs a host login (SSH on Linux). If you can't share credentials, you can apply the setting by hand or deploy a Cloud Agent. Step 6 covers each option.

© 2026 Qualys, Inc. All rights reserved.

01

PHASE 1 · FIND PHP2SHELL

Discover your internet-facing assets

Application: CyberSecurity Asset Management (CSAM) with EASM

YOU NEED	YOU GET	USED IN
Your domains. Optionally your organization name, IP ranges, ASNs and certificate subjects.	An inventory and initial risk indicators for internet-facing hosts and web apps	Step 2 (hosts) and Step 3 (web applications)

EASM finds the hosts, domains, subdomains and web applications your organization owns, using sources such as Shodan, WHOIS and multiple DNS providers. It performs no active scanning and needs no credentials.

Set up discovery

GO TO **CSAM** > Configuration > EASM Configuration

01 Open **CSAM** from the Application Picker, then go to **Configuration > EASM Configuration**.

02 Click **Add Profile** and enter a profile name, for example `PHP2Shell-perimeter`.

03 Under the include filters, add your seeds:

- **Organization:** your legal entity name, as it appears in WHOIS
- **Domain/SubDomain:** primary domains only, for example `example.com`
- Any **IP/Netblock** or **ASNs** you own, and any **certificate subjects** your organization uses

You can also import seeds from a CSV file.

04 To reduce noise from CDN assets, select **CDN** under **Exclude seeds**.

05 Click **Save**. Discovery runs in the background and can take a few hours, depending on volume. Status appears on the EASM Configuration page.

> IMPORTANT
> The free service covers up to 1,000 assets, and the limit applies here. Seed only the domains and addresses you want assessed.

Review what EASM found WHEN STATUS READS COMPLETED

01 Open **Inventory** and turn on the **EASM** switch to see EASM columns such as Open ports, ISP and Domains. The EASM switch is available only in the CSAM Classic view. Use **Group by** to group assets by Organization, Domain/Subdomain and other attributes.

02 Open the **Domains** tab to see every discovered domain and subdomain. Scan these in later steps using DNS tracking.

03 Add any organizations, domains, subdomains or IP addresses that aren't yours to the profile's **Exclude seeds** filter, then click **Save** to schedule another discovery run. To remove assets from your inventory, use the right-click **Quick Actions** menu.

© 2026 Qualys, Inc. All rights reserved.

04 To list the hosts that expose HTTP or HTTPS, enter this query in the asset or domain query control. Then click the download icon above the list to export the results.

CSAM QUERY · WEB-EXPOSED HOSTS

```
openPorts:(detectedService:http or port:[80,443,8000,8080,8443]) or software:(name:iis or name:http or name:nginx or name:php) and not asset.hostingCategory1:`CDN`
```

NOTE

Every EASM asset has a unique IP address. Several assets that share one name or subdomain usually indicate load balancing.

YOU'RE DONE WHEN

You have an exported list of public IPs and FQDNs that expose HTTP or HTTPS, plus the web applications EASM found.

RESULTS APPEAR IN

CSAM > Inventory, and as assets in ETM.

RELATED HELP Configure EASM profile Filter criteria EASM discovery

© 2026 Qualys, Inc. All rights reserved.

02

PHASE 1 · FIND PHP2SHELL

Scan your hosts for PHP2Shell

Application: Vulnerability Management, Detection and Response (VMDR)

YOU NEED	YOU GET	USED IN
Public IPs or FQDNs from Step 1, or your known PHP servers	PHP2Shell detections on hosts, prioritized by TruRisk	Step 4 validation and the Step 5 dashboard

An unauthenticated scan from the Qualys cloud scanners identifies internet-facing hosts that may be vulnerable to PHP2Shell. If your subscription has no scanner appliances, VMDR uses external scanners automatically.

QID	DETECTION
`39033`	PHP2Shell, unauthenticated remote detection
`389102`	PHP2Shell, version-based detection
`45110`	PHP Server Detected (identifies PHP; doesn't confirm the vulnerability)

2a · Add your public hosts

GO TO **VMDR** > Assets > Address Management > New > IP Tracked Hosts

01 Go to **VMDR > Assets > Address Management** and open **Subscription IPs**.

02 Choose **New > IP Tracked Hosts**.

03 Paste the public IPs or ranges from Step 1 (or the IPs of PHP web servers you already know) and save. VMDR can scan only assets that have been added to your subscription.

04 **Optional:** to scan by hostname, a user with the Manager role enables **Scans > Setup > DNS Tracking**. The scan form then accepts FQDNs.

2b · Create a PHP2Shell option profile OPTIONAL

The **Qualys Recommended Option Profile** already includes the PHP2Shell QIDs. A dedicated search list and option profile shortens the scan and keeps the results focused on PHP2Shell.

01 Go to **KnowledgeBase > Search Lists > New > Static List**. Create a list named `PHP2Shell` and add QIDs `45110`, `39033` and `389102`. Add `39036` when it is released.

02 Go to **Scans > Option Profiles > New > Option Profile** and create a profile named `PHP2Shell-External`. On the Scan tab, under Vulnerability Detection, choose **Custom** and add the PHP2Shell search list. Leave authentication disabled and save.

© 2026 Qualys, Inc. All rights reserved.

2c · Launch the scan

GO TO **VMDR** > Scans > Scans > New > Scan

01 Enter a title such as `PHP2Shell external`.

02 Select `PHP2Shell-External` or the Qualys Recommended Option Profile. If a Scanner Appliance list appears, choose **External**.

03 Under **Tell us what to scan**, select **Assets** and enter your IPs, ranges or FQDNs.

04 Optionally, select **Send notification when this scan is finished**.

05 Click **Launch**. When the status in the Scans list reads **Finished**, choose **Quick Actions > View** to review the results.

Review the findings in ETM

GO TO **ETM** > Risk Management > Findings

ETM FINDINGS FILTER · QUALYS VMDR DETECTIONS (QID)

```
finding.qid:[39033, 389102]
```

ETM FINDINGS FILTER · ANY SOURCE (CVE)

```
finding.cveId: CVE-2026-109618 OR finding.cveId: CVE-2026-109619
```

The CVE filter finds PHP2Shell findings from Qualys and non-Qualys sources, including findings imported through the connectors in Phase 3. For the VMDR scan in this step, focus on QID 39033 or 389102.

WHAT YOU SEE	WHAT IT MEANS AND WHAT TO DO
QID 39033 or 389102	Qualys identified a vulnerable PHP version or remotely validated PHP2Shell conditions. Prioritize with TruRisk scores, internet exposure, asset criticality and business context, then validate in Step 4.
QID 45110 only	The host runs PHP, but remote assessment couldn't confirm a vulnerable version. These hosts may still need investigation using the authenticated techniques in Phase 2.

YOU'RE DONE WHEN

You have an inventory of internet-facing PHP systems, initial PHP2Shell findings prioritized by TruRisk, and a list of hosts that need further validation in Phase 2.

RESULTS APPEAR IN

VMDR scan results, ETM > Risk Management > Findings, and the Fightback dashboard.

RELATED HELP Launch a vulnerability scan · Search lists · Choosing an option profile

© 2026 Qualys, Inc. All rights reserved.

03

PHASE 1 · FIND PHP2SHELL

Scan your web applications

Application: TotalAppSec (or WAS)

YOU NEED	YOU GET	USED IN
Web application URLs from Step 1, or public PHP apps you know	PHP2Shell detections on web applications and APIs	ETM findings and the Step 5 dashboard

A host can pass Step 2 while an application on it still exposes PHP2Shell through its upload or session path. TotalAppSec (or WAS) tests the application itself, again from the Qualys cloud scanners, with no appliance.

> **NOTE**
> TotalAppSec is the updated version of Web Application Scanning (WAS). If your subscription still uses WAS, use WAS for this step.

QID	DETECTION
`520310`	PHP Remote Code Execution (RCE) vulnerabilities (PHP2Shell)
`533086`	PHP Remote Code Execution vulnerability (PHP2Shell)
`520404`	PHP session upload progress enabled RCE (CVE-2026-115560)

3a · Add your web applications

GO TO **TotalAppSec (or WAS)** > Web Applications > New Web Application

01 Enter a name and the starting URL, for example `https://www.example.com`. Use the web applications EASM found in Step 1, or any public PHP application you know.

02 Add a tag such as `PHP2Shell` so you can scan the applications as a group.

03 Leave Scanner Appliance set to **External** and save. Repeat for each application, or import a list.

3b · Create a PHP2Shell option profile

01 Create a search list with QIDs `520310`, `533086` and `520404`.

02 Create an option profile and, under detection scope, select the search list you just created.

3c · Launch the scan

GO TO **TotalAppSec (or WAS)** > Scans > New Scan > Vulnerability Scan

01 Name the scan `PHP2Shell web apps`. Choose **Tags** and select `PHP2Shell`, or select applications by name.

02 Select the option profile from 3b and the **External** scanner. Review the settings, then click **Launch**.

© 2026 Qualys, Inc. All rights reserved.

03 Track status in the Scans list. Open the finished scan to see detections for each application.

> **OPTIONAL**
> To check where the scanner will go before testing, first run **Scans > New Scan > Discovery Scan**. A discovery scan only crawls and runs no vulnerability checks.

YOU'RE DONE WHEN

You have application-level PHP2Shell detections alongside the host detections from Step 2. Validate the hosts behind any flagged application in Step 4.

RESULTS APPEAR IN

TotalAppSec (or WAS) scan results, ETM > Risk Management > Findings, and the Fightback dashboard.

RELATED HELP Launch a TotalAppSec scan Search lists Option profiles Discovery scan basics

© 2026 Qualys, Inc. All rights reserved.

04

PHASE 1 · FIND PHP2SHELL

Validate exploitability with TruConfirm

Application: Enterprise TruRisk Management (ETM) · TruConfirm

YOU NEED	YOU GET	USED IN
PHP2Shell findings from Steps 2 and 3	Proof of which hosts are reachable and exploitable	Your fix-first list in Step 6

Steps 2 and 3 identify hosts running potentially vulnerable versions of PHP. TruConfirm shows which of those hosts are exposed and exploitable from outside your network. It also shows whether your existing security controls and mitigations work as expected, so you can separate theoretical risk from what is genuinely open to attack.

The assessment uses a benign upload probe that simulates the first stage of an attack. It creates no files, executes no code and doesn't affect system resources. A successful validation confirms that the vulnerable entry point is reachable and that the `session.upload_progress.enabled=0` mitigation is not in place.

1,539
PHP assets

25
Externally validated targets

In one real-world environment, this process narrowed 1,539 PHP assets to 25 externally validated targets, so remediation could start with the highest-risk systems.

ANONYMIZED DATA

IMPORTANT

TruConfirm assessments come from a dedicated IP pool, separate from the standard Qualys ranges. Don't allowlist these addresses, so the assessment sees what an attacker would see.

Launch the assessment

GO TO **ETM** > TruConfirm > Scan > Launch Scan

Alternatively, go to **Risk Management > Findings > Vulnerabilities**, select the PHP2Shell findings and choose **Launch TruConfirm Assessment**.

01 **Validation source:** select **Scanner Appliance**, then **External** as the scanner type. The assessment runs against the default network, so you don't select one.

02 **Scope:** target the assets from Steps 2 and 3 by IP address, IP range, FQDN or asset tag. Only findings marked **Validation Available** are tested. PHP2Shell (CVE-2026-109618, CVE-2026-109619) supports TruConfirm validation.

03 **Configuration:** keep the default TruConfirm option profile and the default assessment timeout values.

04 **Notification:** enter your email address and select **When scan is finished**.

05 Review the configuration and click **Launch**.

© 2026 Qualys, Inc. All rights reserved.

Review validated findings

GO TO **ETM** > Risk Management > Findings > Vulnerabilities

ETM FINDINGS FILTER · VALIDATED PHP2SHELL (QID)

```
finding.truConfirm.status: "Exploitation Validated" and finding.qid:[39033, 389102]
```

ETM FINDINGS FILTER · VALIDATED PHP2SHELL (CVE)

```
finding.truConfirm.status: "Exploitation Validated" and (finding.cveId: CVE-2026-109618 OR finding.cveId: CVE-2026-109619)
```

TRUCONFIRM STATUS	MEANING	ACTION
Exploit Validated	Entry point reachable, mitigation absent	Fix first in Step 6. The QVSS is raised.
Exploit Ruled Out	Blocked by configuration or controls	Patch on your normal cadence. The QVSS is unchanged or lowered.
Exploit Inconclusive	Could not be determined	Re-run after Step 6, or validate with a Cloud Agent (Phase 2).
Validation Available	Not yet tested	Include it in your next TruConfirm scan.

YOU'RE DONE WHEN

You have evidence of which hosts are both vulnerable and reachable from the internet. Those hosts go to the top of your Step 6 queue.

RESULTS APPEAR IN

ETM Findings (TruConfirm status) and the dashboard's validation widgets.

RELATED HELP Getting started with TruConfirm TruConfirm overview ETM 1.13 release notes

© 2026 Qualys, Inc. All rights reserved.

05

SEE AND FIX

Import the Fightback dashboard

Application: ETM, VMDR or Unified Dashboard

YOU NEED	YOU GET	TIP
The dashboard file from the Qualys blog	One view of your PHP posture, from exposure to remediation	Import it early. It fills in as each scan finishes.

The Qualys Threat Research Unit (TRU) built the PHP2Shell Fightback dashboard to bring the data from Steps 1–4 into one operational view. It shows your PHP footprint, internet-facing exposure, end-of-life PHP deployments, TruConfirm validation results and remediation progress.

DASHBOARD SECTION	WHAT IT SHOWS
PHP footprint	Assets running PHP, with supported deployments separated from end-of-life versions
Exposure and risk	Internet-facing assets, end-of-life software, mod_php deployments and other risk indicators
Remediation prioritization	PHP2Shell findings by operating system, finding age, validation status and remediation state

Import the dashboard

01 Download the dashboard (.zip) and extract the JSON file.

02 In **ETM**, **VMDR** or **Unified Dashboard**, open the **Dashboard** tab.

03 Open the **Tools** menu (or **Manage Dashboards**) and select **Import New Dashboard**.

04 Enter `PHP2Shell Fightback` as the dashboard name, click **Browse** and select the JSON file.

05 To open the dashboard automatically when you enter the application, select **Make this dashboard my default**. Click **Import**.

Keep it one click away OPTIONAL

- **Favorite:** open **Manage Dashboards**, locate the dashboard and select **Mark as Favorite** from the Quick Actions menu.
- **Pin:** open the dashboard selector, click the menu beside the dashboard and choose **Pin Dashboard** (or use the Settings icon on the Dashboard tab). Pinned dashboards stay in the dashboard bar across sessions. You can pin up to five.

> NOTE
> Widgets populate as scans and assessments complete; TruConfirm widgets populate after Step 4. As Qualys releases new PHP detections and remediation guidance, updated dashboards may become available. Re-import the dashboard to get the latest version.

© 2026 Qualys, Inc. All rights reserved.

Query the data directly OPTIONAL

These CSAM queries from the blog work in **CSAM > Inventory > Assets**.

ALL ASSETS WITH PHP INSTALLED

```
(software: ((name: "php")))
```

ASSETS ON END-OF-LIFE PHP (8.1 AND EARLIER)

```
((software: (((name: "PHP") AND (version: (*..8.1))))))
```

END-OF-LIFE PHP ON CRITICAL ASSETS

```
((asset.criticalityScore: [4..*)) AND (software: (((name: "PHP") AND (version: (*..8.1))))))
```

YOU'RE DONE WHEN

The dashboard is imported and pinned, so you can monitor exposure, validation and remediation progress in one place.

FIND IT IN

The Dashboard tab of ETM, VMDR or Unified Dashboard.

RELATED HELP Import and export dashboards Manage dashboards Pin a dashboard

© 2026 Qualys, Inc. All rights reserved.

06

SEE AND FIX

Mitigate or patch, then verify

Application: TruRisk Eliminate

YOU NEED	YOU GET	VERIFY WITH
Findings from Steps 2–4. For scanner-based mitigation, a host login (SSH on Linux).	PHP2Shell mitigated or patched, and a rescan that proves it	The Step 2 and Step 4 rescans, plus the dashboard

Work the queue in this order

1

TruConfirm-validated hosts

Exploit Validated in Step 4. These findings carry an amplified TruRisk QVSS score.

2

Internet-facing end-of-life PHP

PHP 8.1 and earlier, outside regular upstream support.

3

Everything else

Remaining PHP2Shell findings, on your normal cadence.

ETM already sorts this for you: validated findings carry an amplified TruRisk QVSS score, and the Fightback dashboard groups high-risk assets by operating system.

Choose your fix

ANY VERSION · CAN'T PATCH YET · PHP 8.1 OR EARLIER

6a · Mitigate now

Works without a patch, including on end-of-life PHP. Without a Cloud Agent, the scanner needs a host login. Otherwise, apply the setting by hand or deploy an agent (Phase 2).

SUPPORTED BRANCH · PHP 8.2 TO 8.5

6b · Patch

Update to the fixed release, then restart every service that loads PHP.

6a · Mitigate now NO PATCH NEEDED

The Qualys mitigation disables `session.upload_progress`, hardens related session settings on every web-facing PHP runtime on the host, restarts the PHP service and verifies the effective configuration. It removes the confirmed session-lifecycle path.

01 In **ETM**, open the validated PHP2Shell finding (or the asset) and click **Mitigate Now**. This option appears on findings that have a Qualys mitigation.
Alternatively, open the CAR library, search for **PHP2Shell**, import the mitigation script in approved mode, and run it against the hosts from Step 4.

© 2026 Qualys, Inc. All rights reserved.

02 **Execution path:** without a Cloud Agent, choose scanner-based execution. The scanner must log in to change the PHP configuration, so it needs an authentication record for the host (SSH for Linux) and **On-Host Script Execution** enabled in the option profile. If you can't share credentials yet, apply the setting manually (see the table below) or deploy an agent (Phase 2).

03 Check the job log. If it reports that a restart is still required, restart PHP-FPM or Apache manually.

> IMPORTANT
> The mitigation doesn't remove every exploitation path. After the change, test any application that relies on upload progress. Updating PHP is the complete fix.

6b · Patch PHP 8.2–8.5

PHP has released fixed versions for each supported branch:

`8.5.12` `8.4.27` `8.3.36` `8.2.35`

01 In **TruRisk Eliminate**, create a patch job for the vendor update where one is available. Ubuntu's PHP updates (USN-8948-1) deploy with a High reliability rating and no OS reboot.

02 For other distributions, patch through your normal channel using the fixed versions above, then re-run Step 2.

03 Restart every service that loads PHP, or the vulnerable code stays in memory.

PHP 8.1 and earlier are outside regular upstream support. Use a fixed build from your OS or support vendor where one exists, or mitigate (6a).

6c · Verify

01 Re-run the Step 2 VMDR scan and the Step 4 TruConfirm scan. Validated findings should move to **Exploit Ruled Out**, and QID 39033/389102 should clear or show the fixed version.

02 Watch the Fightback dashboard's detection-state widget. Findings move from **Active** to **Fixed**. **Reopened** means a worker still runs the old build.

Manual fallback IF YOU CAN'T RUN ELIMINATE ON A HOST YET

Set these values administratively in `php.ini`, the FPM pool or the Apache configuration, then restart every worker.

SETTING	BLOCKS
`session.upload_progress.enabled = Off`	Confirmed session paths (CVE-2026-109619)
`fatal_error_backtraces = Off` (PHP 8.5)	mod_php backtrace path (CVE-2026-109619)
`memory_limit = -1` via `php_admin_value` `post_max_size = 8M` (32M with uploads)	Attacker-controllable out-of-memory (CVE-2026-109618)
`pm.max_requests = 1` (FPM pool)	State carried over between requests, at a performance cost

© 2026 Qualys, Inc. All rights reserved.

Keep WAF, IPS and EDR signatures for both CVEs enabled as extra layers. The stopgap controls blog lists the vendor rule IDs.

YOU'RE DONE WHEN

Your validated hosts show Exploit Ruled Out on rescan and the dashboard shows their findings as Fixed.

RESULTS APPEAR IN

TruRisk Eliminate job logs, ETM Findings and the Fightback dashboard.

RELATED HELP Stopgap controls blog On-host script execution

© 2026 Qualys, Inc. All rights reserved.

P2

OPTIONAL · AUTHENTICATED COVERAGE

Deploy a Cloud Agent

Application: Cloud Agent

START WITH	YOU GET	ALSO ENABLES
Hosts validated in Step 4, and hosts that reported only QID 45110	The exact PHP packages, versions and install paths on each host	InstaScan, agent-based TruConfirm and agent-based mitigation

External scans assess only what is observable from the internet or your networks. A Qualys Cloud Agent provides host-level visibility, so Qualys can identify the exact PHP packages, versions and installation paths on the system. This matters most for assets where external scanning identified PHP (QID 45110) but couldn't confirm the vulnerability with high confidence.

A Cloud Agent also enables faster detection of newly disclosed vulnerabilities through InstaScan, supports agent-based TruConfirm assessments, and lets TruRisk Eliminate apply mitigations or remediation without scanner-based authentication.

Requirements

Network	Outbound HTTPS (TCP 443) from the host to your Qualys platform URL
Privileges	Local administrator on Windows, or root/sudo on Linux
Footprint	The VMDR configuration adds about 20 MB of download traffic and uses about 100 MB of local disk per host

Deploy the agent

GO TO **Cloud Agent** > Agent Management > Activation Keys > Generate Key

01 Create an activation key named `PHP2Shell`, assign a static tag such as `PHP2Shell`, select the Vulnerability Management and Patch Management modules, and click **Generate**.

02 On the new key, select **Quick Actions > Install Agent**, then choose **Install Instructions** for your target operating system.

03 Download the installer package (.rpm, .deb, .pkg or .exe) and note the installation command shown on the download screen.

04 Install the agent on each target host with elevated privileges. The agent connects to the Qualys platform, retrieves its configuration profile and begins reporting inventory and vulnerability data.

05 Verify that the host appears as **Activated** under **Cloud Agent > Agents** and is visible in **ETM > Assets** with the PHP2Shell tag.

© 2026 Qualys, Inc. All rights reserved.

Validate hosts the external probe couldn't reach

01 Re-run the Step 4 TruConfirm assessment with **Validation source: Cloud Agent**. TruConfirm can then validate hosts the external probe couldn't reach because of network architecture, access controls or other constraints.

02 In Step 6, run the mitigation job as agent-based instead of scanner-based.

WINDOWS: ENABLE DEEP SCAN

On Windows hosts with Cloud Agent 6.2 or later, enable Deep Scan. It finds PHP installed in non-standard directories, on secondary drives and in custom application locations, so duplicate or overlooked PHP binaries don't stay vulnerable after remediation.

ALTERNATIVE: INTERNAL SCANNING WITHOUT AGENTS

To scan internal subnets without agents, deploy a Virtual Scanner Appliance (OVA/VHD) from **VMDR > Scans > Appliances > New**. For internet-facing PHP2Shell exposure, Cloud Agents typically provide the most complete and actionable visibility.

YOU NOW HAVE

Host-level evidence of the PHP version, package inventory and vulnerability status of your highest-priority systems, to target patching, mitigation and validation in Step 6.

RESULTS APPEAR IN

Cloud Agent > Agents, ETM > Assets and ETM Findings.

RELATED HELP Install Cloud Agents Cloud Agent for VMDR

© 2026 Qualys, Inc. All rights reserved.

P3

OPTIONAL

Connect the tools you already run

Application: ETM Connectors

YOU NEED	YOU GET	INSTALLS
A read-only API client in the source tool	PHP2Shell findings from your EDR, XDR, scanner or cloud tools next to Qualys findings	Nothing. Connectors pull data through an API.

Most organizations already hold PHP exposure data in a tool they run today. An ETM connector pulls it in through an API. EDR/XDR, vulnerability scanner and cloud findings for PHP2Shell then appear beside Qualys findings, and TruConfirm can validate them. Your EDR's own PHP2Shell protections can also count as a compensating control in the TruRisk score.

Set up a connector

GO TO **ETM** > Connectors > Integration

01 Find the connector in the marketplace and click **Add** (one time only). Then choose **Manage Connections > Create**.

02 Complete **Profile & Connectivity** and click **Test Connection**.

03 Choose **Data to Sync** (assets and findings) and a schedule.

04 Review and save. The connector runs once immediately, then on schedule.

After the first sync, connector-sourced assets appear in **ETM > Inventory** with their inventory source. **Risk Management > Findings** gains a Source column, so you can filter Qualys and EDR detections for PHP.

Which connector first?

Start with the tools you already run. This list ranks connectors by how much PHP2Shell signal you get for the setup effort. See the full connector catalog.

RANK	CONNECTOR	WHY IT HELPS WITH PHP2SHELL	DOCS
1	**CrowdStrike Falcon (Spotlight)**	Installed PHP packages and CVEs per host on every Falcon server; Falcon's PHP2Shell protections count as a control	Guide
1	**Microsoft Defender for Endpoint V2**	Defender Vulnerability Management inventory and CVEs per machine, Windows and Linux	Guide
2	**Tenable IO**	Direct PHP2Shell plugin results per host; TruConfirm can validate them	Guide
2	**Rapid7 InsightVM**	Findings from your Rapid7 InsightVM estate	Guide

© 2026 Qualys, Inc. All rights reserved.

RANK	CONNECTOR	WHY IT HELPS WITH PHP2SHELL	DOCS
2	**Tanium**	Rich server software inventory; can run the mitigation itself	Guide
3	**AWS Inspector V2**	PHP CVEs on EC2 instances, AMIs and container images	Guide
3	**Wiz (VM Assets)**	Cloud workload PHP CVEs, where end-of-life images hide	Guide
3	**Microsoft Defender for Cloud (VM Assets)**	Azure VM PHP findings	Guide
3	**Orca Security (VM Assets)**	Agentless cloud workload PHP CVEs	Guide
4	**SentinelOne, Cortex XDR, Cybereason, Symantec**	Endpoint coverage; PHP package data on Linux servers is less consistent	Docs
4	**Burp Suite, Veracode DAST, Checkmarx DAST**	Confirm that an application sits on vulnerable PHP; rarely give the version	Docs

RELATED HELP Connector catalog CrowdStrike Endpoint Security connector Defender for Endpoint V2 connector

© 2026 Qualys, Inc. All rights reserved.

REFERENCE

QIDs, fixed versions and support

PHP2Shell QIDs used in this guide

QID	TITLE	APPLICATION	STEP
39033	PHP2Shell, unauthenticated remote detection	VMDR	2
389102	PHP2Shell, version-based detection	VMDR	2
45110	PHP Server Detected (inventory only; doesn't confirm a CVE)	VMDR	2
39036	PHP session upload progress RCE (CVE-2026-115560), to be released	VMDR	2
520310	PHP Remote Code Execution (RCE) vulnerabilities (PHP2Shell)	TotalAppSec (or WAS)	3
533086	PHP Remote Code Execution vulnerability (PHP2Shell)	TotalAppSec (or WAS)	3
520404	PHP session upload progress enabled RCE (CVE-2026-115560)	TotalAppSec (or WAS)	3

The PHP2Shell blog lists every related QID, including the distribution vendor advisories.

Fixed PHP releases

`8.5.12` `8.4.27` `8.3.36` `8.2.35`

PHP 8.1 and earlier are outside regular upstream support. Use a fixed build from your OS or support vendor where one exists, or mitigate (Step 6a). Distribution backports can keep older version numbers, so check your vendor's advisory.

Further reading

- PHP2Shell: Find, Mitigate, and Patch Now · Qualys Threat Research Unit
- Can't Patch PHP2Shell Yet? Build a Stopgap with the Controls You Own · Qualys blog
- PHP2Shell emergency briefing · on demand
- PHP2Shell free service

Support during your free service

Qualys Support	Help with your account and the applications in this guide
Qualys Documentation	Release notes, user guides and more for every Qualys application
Qualys Training & Certification Center	Free training on Qualys applications

© 2026 Qualys, Inc. All rights reserved.



About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide.

qualys.com

© 2026 Qualys, Inc. All rights reserved. Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.