Qualys Threat Research Unit

Oct 2026

This Month's Update

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

10 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

PHP2Shell: Find, Mitigate, and Patch Now (CVE-2026-109618, CVE-2026-109619)

Measure, communicate, and eliminate your cyber risk—before it escalates into a crisis.

PHP2Shell: Find, Mitigate, and Patch Now (CVE-2026-109618, CVE-2026-109619)

PHP released fixes on October 21, 2026 for two critical bugs known as PHP2Shell (CVE-2026-109618 and CVE-2026-109619). They let an attacker run code on a server without logging in. Across more than 10,000 organizations, Qualys found 167 million PHP installations, and only 0.37% were patched in the first 24 hours. The flaws are now being actively exploited — CISA added both to its Known Exploited Vulnerabilities catalog on October 26 —

and Cloudflare has seen attackers trying to slip past its filters. If you run PHP 8.2 through 8.5, update now.

More than 70% of the installs Qualys found are on PHP 8.1 or older, end-of-life versions with no official fix. Check with your OS vendor for a backported patch, or isolate the system and plan an upgrade. Qualys can help you find every PHP install, put a temporary safeguard in place while you patch, and confirm the fix.

Read the full details on our blog.

Free PHP2Shell Service from Qualys

Not sure where PHP2Shell sits in your environment? Qualys is offering a free service that scans your internet-facing assets from the cloud, no agents needed, shows which PHP servers attackers can actually exploit, and lets you mitigate the ones you can't patch yet, including EOL versions PHP will never fix. Free for 15 days, up to 1,000 assets.

Get the free service

For more in-depth information, visit the Qualys ThreatPROTECT page and subscribe to receive the latest updates on threats and vulnerabilities.

These vulnerabilities pose significant risks to your systems. To understand and address these critical threats, get your **personalized TruRisk Report**. **Contact your Technical Account Manager today to get yours.**

October's Must-Know Risks

PHP Remote Code Execution via Out-of-Memory Corruption Vulnerability

CVE-2026-109618
QID:389102,39033

QVSS **9.4**

PHP Remote Code Execution via Stale Global State Vulnerability

CVE-2026-109619
QID:389102,39033

QVSS **9.5**

FortiMail Path Traversal and Improper Neutralization of NULL Byte Vulnerability

CVE-2026-104286
QID:388879

QVSS **9.5**

Cisco Secure Email Gateway Arbitrary File Write Vulnerability

CVE-2026-76519
QID:317944

QVSS **9.5**

Atlassian Multiple Products Arbitrary File Access Vulnerability

CVE-2026-21589
QID:735708,388907,735703,735702,388903

QVSS **9.5**

Windows Shell Security Feature Bypass Vulnerability

CVE-2026-90351
QID:92486,92482

QVSS **9.5**

Citrix NetScaler ADC/Gateway Memory Overflow (DoS) Vulnerability

CVE-2026-88779
QID:388894

QVSS **9.5**

Ivanti Connect Secure Authentication Bypass Vulnerability

CVE-2026-104935
QID:735730,735728

QVSS **9.5**

PAN-OS: Authenticated Remote Code Execution (RCE) in the Management Interface

CVE-2026-0322
QID:735740

QVSS **9.5**

Node.js Brotli Decoder Out-of-Bounds Write Remote Code Execution Vulnerability

CVE-2026-111497
QID:389117

QVSS **5.5**

Node.js Patches Brotli Remote Code Execution Flaw

Node.js released fixes on October 21, 2026 for 10 security bugs, the worst of which — CVE-2026-111497, a flaw in how Node.js decompresses Brotli data — lets an attacker run code on a server. CISA added it to its Known Exploited Vulnerabilities catalog on October 27, confirming it's being actively exploited. Across the installations Qualys scanned, fewer than 2 in 100 have been patched so far, and more than 93% of Node.js installations remain either unpatched or on a version with no fix available. These bugs live inside the Node.js runtime itself, not in an add-on package, so a normal dependency check won't catch them. If you're on Node.js 22, 24, or 26, update to the latest patched release right away.

More than half the installs Qualys found are on end-of-life Node.js versions (25, 23, 20, or older) with no fix coming — move those to a supported line as soon as possible. Qualys can help you find every vulnerable Node.js runtime, including ones hiding in containers or unusual folders, and confirm once you're patched.

Read the full details on our blog.

Cloud Security Snapshot: Key Misconfigurations

Unveiled by our expert analysts: the top risk combinations threatening your cloud today. Identify critical cybersecurity threats facing your organization and learn the strategies to mitigate them. Act fast—secure your cloud before it's too late.
The following percentages reflect the number of resources across all customers that have these misconfigurations.

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
Ensure that ALB drops HTTP headers	86.00%
Ensure EBS default encryption is enabled with customer managed key	86.00%
Ensure public facing ALB are protected by WAF	69.00%
Ensure that NLB balancer listener is not using unencrypted protocol	72.00%
Ensure to update the Security Policy of the Network Load Balancer	28.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure that the endpoint protection for all Virtual Machines is installed	97.00%
Ensure Storage for Critical Data are Encrypted with Customer Managed Keys	94.00%
Ensure that Diagnostic logs are enabled in Virtual Machine Scale Sets	70.00%
Ensure that all Attached VM Disks are encrypted with Customer Managed Key (CMK)	96.00%
Ensure that Virtual Machine Scale Sets have encryption at host enabled	93.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure that your production Google Cloud virtual machine instances are not preemptible	26.00%
Ensure that deletion protection is enabled for your Google Cloud virtual machine (VM) instances	98.00%
Ensure that your virtual machine (VM) instance disks are encrypted using Customer-Managed Keys (CMKs)	90.00%
Ensure that instances are not configured to use the default service account with full access to all Cloud APIs	46.00%
Ensure Block Project-wide SSH keys enabled for VM instances	89.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure customer created Customer Managed Key (CMK) is rotated at least annually	31.00%
Ensure secret reuse rule should be configured	92.00%
Ensure secret auto rotation should be enabled	99.00%
Ensure no policies have manage-all resources permission in a compartment	19.00%
Ensure only required Compute Instances have been assigned with Public IP	13.00%

These misconfigurations pose significant risks to your cloud. To understand and address these critical issues, **get your Cloud TruRisk Insight Report**. This report identifies the misconfigurations that pose risks and provides actionable steps to remediate them. **Contact your Technical Account Manager today to get your personalized report and secure your cloud**.

Stay protected by leveraging Qualys' comprehensive vulnerability detection and management.

Reach out to your Technical Account Manager today to discuss the fastest ways to remediate these critical risks and strengthen your security posture. Don't wait; proactive steps now can prevent costly breaches later.

Thank you

for being part of our October newsletter! We hope these insights empower you to enhance your security posture. Get ready for next month's edition, filled with the latest updates and expert threat research tips.

We value your input; what topics would you like us to explore next? Drop us a line anytime at researchnewsletter@qualys.com. Until then, stay safe and secure!

Qualys.

© 2026 Qualys, Inc. All rights reserved. Privacy Policy, Accessibility, Notice at Collection, Trust, Cookie Consent.