Qualys Threat Research Unit

June 2026

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

12 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

Qualys Joins Anthropic's Project Glasswing to Advance Cybersecurity in the Frontier AI Era

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

June's Must-Know Risks

Oracle PeopleSoft Remote Code Execution Vulnerability

CVE-2026-35273
QID:387569

QVSS **10**

Check Point VPN Auth Bypass Vulnerability

CVE-2026-50751
QID:387569

QVSS **10**

Google Chrome Zero-day Vulnerability

CVE-2026-11645
QID:387568

QVSS **9.5**

Ivanti Sentry Command Injection Vulnerability

CVE-2026-10520
QID:734395

QVSS **9.5**

PAN-OS GlobalProtect Auth Bypass Vulnerability

CVE-2026-0257
QID:734231

QVSS **9.5**

Cisco Catalyst SD-WAN Manager EoP Vulnerability

CVE-2026-20245
QID:317857

QVSS **9.5**

Cisco Catalyst SD-WAN Manager Arbitrary File Write Vulnerability

CVE-2026-20262
QID:317858

QVSS **9.5**

Splunk Enterprise Arbitrary File Creation & Truncation Vulnerability

CVE-2026-20253
QID:387594

QVSS **9.5**

HTTP.sys RCE Vulnerability

CVE-2026-47291
QID:92408

QVSS **7.2**

Windows ADDS RCE Vulnerability

CVE-2026-45648
QID:92404

QVSS **3.5**

Windows Kernel Remote Code Execution Vulnerability

CVE- 2026-45657
QID:92405,92404

QVSS **6.5**

Microsoft Outlook and Word RCE Vulnerability

CVE- 2026-45456
QID:110528,110527

QVSS **3.5**

For more in-depth knowledge and details, visit 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 TAM today to get yours.**

Meeting CISA BOD 26-04: Why Federal Agencies Need a Risk Operations Center

Released June 10, 2026, CISA's Binding Operational Directive (BOD) 26-04 pushes federal agencies away from blanket patching toward risk-based vulnerability management. Because AI has compressed exploitation timelines from weeks to hours, agencies must now rank vulnerabilities by real-world exploitability, exposure, KEV status, and mission impact, then remediate the highest-risk ones within 72 hours. Qualys answers with a Risk Operations Center, a closed loop that ties detection and prioritization directly to validated, automated remediation and measurable risk reduction. Built on VMDR, ETM, and TruRisk Eliminate, the ROC helps agencies focus on the handful of vulnerabilities attackers can actually reach and prove that exposure is shrinking.

Read our blog **here**

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	87%
Enable EBS default encryption with a customer-managed key	88%
Ensure public-facing ALBs are protected by WAF	69%
Ensure NLB listeners do not use unencrypted protocols	74%
Ensure the Network Load Balancer security policy is updated	95%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure endpoint protection is installed on all VMs	98%
nsure critical data storage uses Customer-Managed Keys	91%
Ensure diagnostic logs are enabled for VM Scale Sets	99%
Ensure automatic OS image patching is enabled for VM Scale Sets	99%
Ensure host encryption is enabled for VM Scale Sets	91%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure production Google Cloud VMs are not preemptible	19%
Enable CSEK encryption for critical VM disks	96%
Encrypt VM disks using Customer-Managed Keys	89%
Disable full Cloud API access for default service accounts	50%
Ensure VM instances block project-wide SSH keys	91%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure Customer-Managed Keys are rotated annually	31%
Ensure secret reuse prevention is configured	90%
Ensure secret auto-rotation is enabled	98%
Ensure no compartment policies grant manage-all-resources	13%
Ensure only required compute instances have public IPs	28%

These misconfigurations pose significant risks to your cloud. To understand and address these critical issues, **get your Cloud TruRisk Insight Report**. This report identifies which misconfigurations are causing risks and provides actionable steps to remediate them. **Contact your TAM today to get your personalized report and secure your cloud**.

Qualys Joins Anthropic's Project Glasswing to Advance Cybersecurity in the Frontier AI Era

Qualys has accepted an invitation to join Anthropic's Project Glasswing and OpenAI's Trusted Access for Cyber, two programs where technology and cybersecurity leaders study how advanced AI reshapes security and how to deploy it responsibly. Most of the industry is focused on how attackers might use AI. Qualys sees the bigger prize on the defensive side: using frontier AI to replace slow, manual review with continuous, machine-speed risk reduction. That perspective is grounded in scale, with more than 200 million Qualys agents deployed worldwide. Early on, the company is applying frontier AI to strengthen its own software assurance and speed vulnerability discovery, working toward autonomous risk management delivered through the Qualys ETM and ROC platform.

For more information, please **read our blog**.

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

Reach out to your Technical Account Manager (TAM) 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 June 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.