Qualys Threat Research Unit

November 2025

This Month's Update

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

7 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

0-Day O: AI Attacks and the End of the "Forgiving Internet"

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

November's Must-Know Risks

MS Windows Server Update RCE

CVE-2025-59287
QID: 92326

QVS 100

Fortinet FortiWeb Zero-day

CVE-2025-64446
QID: 733406, 733407

QVS 95

Adobe Magento Improper Input Validation

CVE-2025-54236
QID: 733319, 530559

QVS 95

Gladinet Triofox Improper Access Control

CVE-2025-12480
QID: 386020, 733415

QVS 95

Windows Kernel Elevation of Privilege

CVE-2025-62215
QID: 92332, 92329

QVS 95

Google Chromium V8 Type Confusion

CVE-2025-13223
QID: 386014

QVS 95

FortiNet FortiWeb OS Command Injection

CVE-2025-58034
QID: 44820

QVS 95

Cisco Unified Contact Center Express RCE

CVE-2025-20354, CVE-2025-20358
QID: 317749

QVS 65

Microsoft Office RCE

CVE-2025-62199
QID: 110510

QVS 35

Windows CLFS driver out-of-bounds

CVE-2025-60709
QID: 92332, 92329

QVS 35

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 Technical Account Manager today to get yours.**

Cloud Security Snapshot: Key Misconfigurations

Unveiled by our expert analysts: the top risk combinations threatening your cloud today. Discover critical cybersecurity dangers facing your organization and master the strategies to neutralize them. Act fast—secure your cloud before it's too late.

The following percentages reflect how many resources across all customers have these misconfigurations.

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
Ensure access keys unused for 90 days or greater are disabled	75.00%
Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	90.00%
Ensure RDS MS SQL instance enforces encrypted connections only	87.00%
Ensure Redshift clusters are not publicly accessible	18.00%
Ensure that DocumentDB Instances certificates are rotated	96.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure no SQL Servers allow ingress from Internet (ANY IP)	53.00%
Ensure that public network access is disabled in Managed Disks	40.00%
Ensure that Cognitive Services enable data encryption with customer-managed keys	98.00%
Ensure that Storage Account Access Keys are Periodically Regenerated	83.00%
Ensure that Azure Storage account access is limited only to specific IP address(es)	72.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure Block Project-wide SSH keys enabled for VM instances	92.00%
Ensure no roles that enable to impersonate and manage all service accounts are used at a project level	96.00%
Ensure that BigQuery Dataset is encrypted with Customer-managed key	90.00%
Ensure that Default service account is not used for the cloud function	43.00%
Ensure No Cloud Run Service is Publicly Accessible	21.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure no Object Storage buckets are publicly visible	38.00%
Ensure no security lists allow ingress from 0.0.0.0/0 or ::/0 to port 22	46.00%
Ensure MFA is enabled for all users with a console password	70.00%
Ensure user API keys rotate within 90 days or less	93.00%
Ensure Object Storage Buckets are encrypted with a Customer Managed Key CMK	61.00%

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

Zero-Day Zero: AI Attacks and the End of the "Forgiving Internet"

AI-powered attackers can now scan the internet, identify weaknesses, craft exploits, move laterally, and exfiltrate data with almost no human involvement. A recent nation-state campaign demonstrated how an AI agent chained together reconnaissance, vulnerability discovery, exploit generation, and credential abuse in minutes — actions that once took human operators days or weeks. This surge in autonomous attack speed means every stray service, outdated system, or misconfiguration becomes an immediate liability. The shift demands continuous asset visibility, aggressive hardening, strict zero-trust enforcement, and the adoption of defensive AI capable of responding at machine speed. For more details, read our blog.

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 November 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.