Qualys Threat Research Unit

September 2025

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

4 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

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

September's Must-Know Risks

Citrix NetScaler ADC and Gateway

CVE-2025-7775
QID: 384699

QVS 95

Apple iOS, iPadOS, and macOS

CVE-2025-43300
QID: 384609, 384608, 384607

QVS 95

SAP S/4HANA Code Injection

CVE-2025-42957
QID: 385079

QVS 95

TP-Link Router Vulnerabilities

CVE-2025-9377
QID: 733151

QVS 95

Sitecore Experience Platform RCE

CVE-2025-53690
QID: 385059

QVS 92

Cisco Secure FW Management RCE

CVE-2025-20265
QID: 317674

QVS 95

Microsoft HPC Pack RCE

CVE-2025-55232
QID: 385091

QVS 65

Microsoft Office RCE

CVE-2025-54910
QID: 110505

QVS 35

Windows NTLM Elevation of Privilege

CVE-2025-54918
QID: 92307, 92305

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 (%)
Multi-factor authentication (MFA) is enabled for all IAM users that have a console password	59.00%
Amazon OpenSearch Service domains are publicly accessible	26.00%
Access Keys unused for 90 days or greater are not disabled	72.00%
Security groups allow ingress from 0.0.0.0/0 to port 22	16.00%
Expired certificates are removed from Certificate Manager (ACM)	28.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Expiration Date is not set for all Secrets in RBAC Key Vaults	65.00%
Cognitive Services do not use private links	85.00%
Storage for Critical Data are Encrypted with Customer Managed Keys	88.00%
App Service Authentication is not set on Function Apps	94.00%
Public network access is not disabled or restricted in Cognitive Services accounts	69.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Project has Service Account with Admin Privileges	32.00%
User-managed/external keys for service accounts are rotated every 90 days or less	92.00%
GCP Storage bucket is encrypted not using customer-managed key	88.00%
KMS encryption keys are not rotated within a period of 90 days	32.00%
BigQuery Dataset is not encrypted with Customer-managed key	92.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Object Storage buckets are publicly visible	38.00%
Network security groups allow ingress from 0.0.0.0/0 or ::/0 to port 22	44.00%
User API keys rotate within 90 days or less	90.00%
MFA is enabled for all users with a console password	75.00%
Boot volumes are encrypted with Customer Managed Key (CMK)	96.00%

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**.

Shaping the Future of Cyber Risk Management: QSC Evolves to ROCon

For over two decades, the Qualys Security Conference (QSC) has brought the cybersecurity community together to share insights and explore new solutions. This year, we are proud to announce QSC's transformation from a user summit into a premier industry event: the very first Risk Operations Conference (ROCon).

The Risk Operations Center (ROC) establishes a new frontier in risk management – aligning cybersecurity strategy with measurable business outcomes. ROCon will convene the global security community to embrace this vision and shape the future of cyber risk.

Join us as we usher in the new paradigm of cybersecurity
Read the blog for the details.

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 September 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!