Qualys Threat Research Unit

JULY 2025

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

6 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

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

July's Must-Know Risks

Anthropic MCP Inspector RCE

CVE-2025-49596
QID: 732720, 5004419, 530238

QVS 100

Fortinet FW Unauth SQLi

CVE-2025-25257
QID: 44706, 732762

QVS 100

Citrix NetScaler ADC & Gateway

CVE-2025-6543
QID: 383418

QVS 95

NetScaler Disclosure CitrixBleed 2

CVE-2025-5777
QID: 732730, 530199, 383389

QVS 95

Google Chrome Zero-day

CVE-2025-6554
QID: 383440

QVS 95

WingFTP Critical RCE

CVE-2025-47812
QID: 383441, 530239

QVS 95

MS SP Untrusted Data Deserialization

CVE-2025-53770
QID: 110501

QVS 95

Cisco Unified CM Static SSH Creds

CVE-2025-20309
QID: 317668

QVS 65

Win SPNEGOEX Security RCE

CVE-2025-47981
QID: 92287

QVS 65

MS SQL Server Information Disclosure

CVE-2025-49719
QID: 383511

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 (%)
Secrets should be auto rotated after not > 90 days	98.00%
Usage of root account is monitored	95.00%
Network ACLs allow ingress from 0.0.0.0/0 to port 3389	95.00%
Access keys unused for 90 or more days are disabled	74.00%
Encrypt the destination S3 bucket in the audit logging account	95.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
App Service Authentication is set on Function Apps	97.00%
Function app has Client Certificates set to On	95.00%
VM disks for critical VMs are encrypted with CSEK	93.00%
Public N/W Access is Disabled for storage accounts	89.00%
Container Registry disallows unrestricted N/W Access	82.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
API Keys are rotated every 90 days	84.00%
GCP Storage bucket is encrypted using CMK	79.00%
BigQuery Table is encrypted with CMK	87.00%
Enable Private Google Access for all subnetworks in the VPC	91.00%
Ensure that PostgreSQL instances are CMK-encrypted	88.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
DB Systems DB is encrypted using CMK	99.00%
Disable Compute Instance Legacy Metadata Service EP	95.00%
Enable in-transit encryption on Compute Instance Boot Vol	87.00%
Restrict resource permissions to the tenancy admin group.	93.00%
User Auth Tokens rotate within 90 days or less	94.00%

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**.

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 July 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.