Qualys Threat Research Unit

Aug 2025

This Month's Update

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

4 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

2 Pwnie Awards

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

August's Must-Know Risks

WinRAR Path Traversal

CVE-2025-8088
QID: 383966

QVS 95

Trend-Micro Apex One Zero-Day

CVE-2025-54948
QID: 383740

QVS 95

PaperCut NG/MF Vulnerability

CVE-2023-2533
QID: 383707, 530341

QVS 95

CrushFTP Authentication Bypass

CVE-2025-54309
QID: 383614

QVS 92

Adobe Experience Manager Zero-Day

CVE-2025-54253
QID: 732858

QVS 72

Windows GDI+ RCE

CVE-2025-53766
QID: 92297, 92295

QVS 65

Windows Graphics Component RCE

CVE-2025-50165
QID: 92297, 92295

QVS 65

Windows Kerberos EoP

CVE-2025-53779
QID: 92297

QVS 42

Microsoft Office RCE

CVE-2025-53731/ CVE-2025-53740
QID: 110503

QVS 35

Microsoft Sharepoint RCE

CVE-2025-49712
QID: 110504

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.

Dual Win at Prestigious Pwnie Awards

Qualys' Threat Research Unit (TRU) was honored with dual win at prestigious Pwnie Awards for groundbreaking cybersecurity research and reinforcing its leadership in global cybersecurity innovation.

- **Pwnie for Best RCE:** regreSSHion (CVE-2024-6387) — a pre-auth, no-interaction RCE in OpenSSH's default server caused by a rare signal-handler race leading to exploitable heap corruption, granting full root privileges and posing a significant security risk; the first in ~20 years.
- **Pwnie for Epic Achievement:** two OpenSSH bugs — CVE-2024-6387 and CVE-2025-26465, a client machine-in-the-middle flaw with FreeBSD vulnerable by default for ~10 years.

Beyond the trophies, our blog post explains what OpenSSH bugs reveal about patching. We analyzed over 8.8 million anonymized vulnerability lifecycle events across enterprise environments, half of fixes land in 24 hours—risk lingers in the long tail. Read the blog for the details.

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 (%)
Block new public bucket policies for an account is set to true	61.00%
Secrets should be auto rotated after not more than 90 days	98.00%
Network ACLs allow ingress from 0.0.0.0/0 or ::/0 to port 22	93.00%
EBS default encryption is enabled with customer managed key	78.00%
Block public sharing setting is ON for the documents in all regions	82.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Custom subscription Administrator Roles exist	45.00%
Storage accounts allow Blob public access	28.00%
Expiration Date is not set for all Secrets in RBAC Key Vaults	62.00%
MariaDB Server allow ingress from Internet (ANY IP)	70.00%
Azure CosmosDB does allow access from all networks	82.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
BigQuery Dataset is not encrypted with Customer-managed key	91.00%
Cloud SQL - Mysql DB instance requires all incoming connections to use SSL	62.00%
BigQuery Table is not encrypted with Customer-managed key	93.00%
Service accounts' user-managed/external keys aren't rotated every 90 days or less	92.00%
Project has Service Account with Admin Privileges	32.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Boot volumes are not encrypted with CMK	96.00%
IAM password policy requires minimum length of 14 or greater	95.00%
Secret auto rotation should be enabled	94.00%
DB Systems Network Security Groups don't restrict access to and from the DB.	86.00%
File Storage Systems are not encrypted with CMK	85.00%

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 August 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!