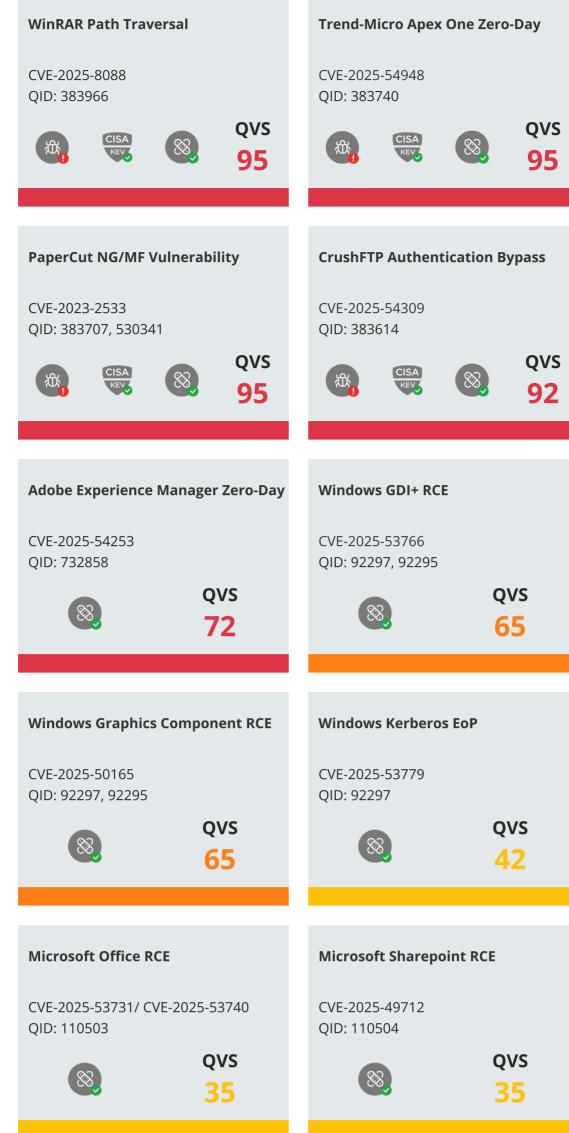




cyber risk—before it escalates into a crisis.

Measure, communicate, and eliminate your





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.

For more in-depth knowledge and details, visit **Qualys ThreatPROTECT** page and

subscribe to receive the latest updates on threats and vulnerabilities.

Dual Win at Prestigious Pwnie Awards

Pwnie Awards for groundbreaking cybersecurity research and reinforcing its leadership in global cybersecurity innovation. • Pwnie for Best RCE: <u>regreSSHion (CVE-2024-6387)</u> — 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

Qualys' Threat Research Unit (TRU) was honored with dual win at prestigious

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.

before it's too late.

than 90 days

managed key

documents in all regions

to port 22

have these misconfigurations.

Amazon Web Services (AWS)

Network ACLs allow ingress from 0.0.0.0/0 or ::/0

EBS default encryption is enabled with customer

Block public sharing setting is ON for the

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.



The following percentages reflect how many resources across all customers

Cloud Security Snapshot: Key

Misconfigurations

Resources Misconfiguration Affected (%) Block new public bucket policies for an account is 61.00% Secrets should be auto rotated after not more 98.00%

93.00%

78.00%

82.00%

95.00%

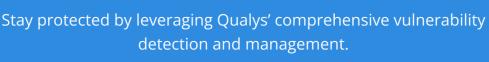
Microsoft Azure Resources Affected Misconfiguration (%) **Custom subscription Administrator Roles exist** 45.00% Storage accounts allow Blob public access 28.00% **Expiration Date is not set for all Secrets in RBAC** 62.00% MariaDB Server allow ingress from Internet (ANY 70.00% Azure CosmosDB does allow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

	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%

Secret auto rotation should be enabled 94.00% **DB Systems Network Security Groups don't restrict** 86.00% access to and from the DB. 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

IAM password policy requires minimum length of

14 or greater



secure your cloud.

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 <u>researchNewsletter@qualys.com</u>. Until then, stay safe and secure!



Accessibility. Notice at Collection. Trust. Cookie Consent.