



Stay Secure with Qualys This month: critical vulnerabilities, cloud misconfigurations, and

Qualys TRU's two OpenSSH finds.



Qualys coverage contains these severe vulnerabilities.

March's Must-Know Risks

CVE-2024-53704 QID: 732253, 732163

Authentication Vulnerability

SonicWall SonicOS SSLVPN Improper





QVS

CVE-2025-0108 QID: 732239, 732237

Authentication Bypass Vulnerability

Palo Alto Networks PAN-OS



Following Vulnerability



QVS

CVE-2025-24200 QID: 610632, 610631

Apple iOS and iPadOS Incorrect

Authorization Vulnerability





Microsoft Windows Ancillary



CVE-2025-21391 QID: 92215, 92213

Microsoft Windows Storage Link



Vulnerabilities

Management Multiple

SimpleHelp Remote Monitoring and

CVE-2025-21418 QID: 92215, 92213 QVS

CVE-2025-22224 to CVE-2025-22226

Function Driver for WinSock Heap-

Based Buffer Overflow Vulnerability





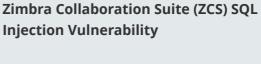
Fusion Vulnerabilities

QID: 382910, 216336, etc



VMware ESXi, Workstation, and

CVE-2024-57726 to CVE-2024-57728 QID: 732189, 152661, etc



CVE-2025-25064

QID: 382807, 152713

Apple Multiple Products Use-After-

Free Vulnerability

CVE-2024-24085

QVS

QID: 732234, 732235, etc

Ivanti Multiple Vulnerabilities

CVE-2025-22467, CVE-2024-10644 +

QVS

securely encrypted at rest

customer-managed key

topics

managed key

managed key

port 22/3389

users

Managed Key (CMK)

Amazon API Gateway APIs are not accessible

through private API endpoints in all regions

Container Registries are not encrypted with a

Public Network Access is enabled in Azure Event Grid

User-managed/External keys for service accounts

BigQuery Table is not encrypted with Customer-

Security Lists allow ingress from 0.0.0.0/0 or ::/0 to

Boot volumes are not encrypted with Customer

API keys are created for tenancy administrator

MFA is not enabled for all users with a console

Vulnerabilities

legitimate access.

Block Project-wide SSH keys disabled for VM

are not rotated every 90 days or less



8 More CVEs

Misconfigurations

QID: 610628, 382740, etc



Unveiled by our expert analysts: the top risk combinations threatening your cloud today. Discover critical cybersecurity





93%

82%

98%

96%

93%

99%

91%

45%

96%

25%





dangers facing your organization and master the strategies to neutralize them. Act fast—secure your cloud before it's too late.

Cloud Security Snapshot: Key

Amazon Web Services (AWS) Resources Misconfiguration Affected (%) **ECR repositories are not encrypted using KMS** 94% Data stored in the Sagemaker Endpoint is not

MFA is not enabled for the root user account 30% Access keys unused for 90 days or greater are not 82% disabled **Microsoft Azure** Resources Misconfiguration Affected (%) **Storage logging is not enabled for Blob/Queue/Table** 97% service for read, write and delete requests

Kubernetes Services Management API server is not 62% configured with restricted access Firewall rules allow internet access for Azure Redis 82% Cache **Google Cloud Platform (GCP)** Resources Misconfiguration Affected (%) Storage bucket is not encrypted using customer-97%

instances Application-Layer secret encryption disabled for 83% **Kubernetes cluster Oracle Cloud Infrastructure (OCI)** Resources Misconfiguration Affected (%) **User Customer Secret keys are not rotated within** 98% 90 days or less

91% Note: Percentages reflect how many resources across all customers, have these misconfigurations. **Protect Your Cloud:** Fix these common issues to secure your environment. Reach out to your TAM for expert support. **Qualys TRU has discovered two** vulnerabilities in OpenSSH

Act Now to Protect Your Systems from OpenSSH

The Qualys Threat Research Unit (TRU) has uncovered two vulnerabilities in OpenSSH: CVE-2025-26465 and CVE-2025-26466. These flaws expose your SSH sessions to risks like credential theft, session hijacking, or service disruptions.

CVE-2025-26465: Attackers can intercept SSH connections, compromising sensitive data.

CVE-2025-26466: Triggers pre-authentication denial-of-service, blocking

infrastructure. Act fast—patch today! For a deep dive into these vulnerabilities and expert insights, visit our blog.

Take Action: Upgrade to OpenSSH 9.9p2 immediately to safeguard your

Stay protected by leveraging Qualys' comprehensive vulnerability detection and management. For more in-depth knowledge and details,

Reach out to your Technical Account Manager (TAM) 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.

visit **Qualys ThreatPROTECT** page and subscribe to receive the latest updates on threats and vulnerabilities.

Thank you

for being part of our March 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!

Qualys.

© 2025 Qualys, Inc. All rights reserved. Privacy Policy.

Accessibility. Notice at Collection. Trust. Cookie Consent.