Qualys Threat Research Unit

MARCH 2025

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

Stay Secure with Qualys

This month: critical vulnerabilities, cloud misconfigurations, and Qualys TRU's two OpenSSH finds.

March's Must-Know Risks

Qualys coverage contains these severe vulnerabilities.

SonicWall SonicOS SSLVPN Improper Authentication Vulnerability

CVE-2024-53704
QID: 732253, 732163

QVS
95

Palo Alto Networks PAN-OS Authentication Bypass Vulnerability

CVE-2025-0108
QID: 732239, 732237

QVS
95

Apple iOS and iPadOS Incorrect Authorization Vulnerability

CVE-2025-24200
QID: 610632, 610631

QVS
95

Microsoft Windows Storage Link Following Vulnerability

CVE-2025-21391
QID: 92215, 92213

QVS
95

Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability

CVE-2025-21418
QID: 92215, 92213

QVS
95

SimpleHelp Remote Monitoring and Management Multiple Vulnerabilities

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

QVS
95

VMware ESXi, Workstation, and Fusion Vulnerabilities

CVE-2025-22224 to CVE-2025-22226
QID: 382910, 216336, etc

QVS
95

Zimbra Collaboration Suite (ZCS) SQL Injection Vulnerability

CVE-2025-25064
QID: 382807, 152713

QVS
72

Ivanti Multiple Vulnerabilities

CVE-2025-22467, CVE-2024-10644 + 8 More CVEs
QID: 732234, 732235, etc

QVS
65

Apple Multiple Products Use-After-Free Vulnerability

CVE-2024-24085
QID: 610628, 382740, etc

QVS
N/A

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.

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
ECR repositories are not encrypted using KMS	94%
Data stored in the Sagemaker Endpoint is not securely encrypted at rest	93%
Amazon API Gateway APIs are not accessible through private API endpoints in all regions	82%
MFA is not enabled for the root user account	30%
Access keys unused for 90 days or greater are not disabled	82%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Storage logging is not enabled for Blob/Queue/Table service for read, write and delete requests	97%
Container Registries are not encrypted with a customer-managed key	98%
Public Network Access is enabled in Azure Event Grid topics	96%
Kubernetes Services Management API server is not configured with restricted access	62%
Firewall rules allow internet access for Azure Redis Cache	82%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Storage bucket is not encrypted using customer-managed key	97%
User-managed/External keys for service accounts are not rotated every 90 days or less	93%
BigQuery Table is not encrypted with Customer-managed key	99%
Block Project-wide SSH keys disabled for VM instances	91%
Application-Layer secret encryption disabled for Kubernetes cluster	83%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
User Customer Secret keys are not rotated within 90 days or less	98%
Security Lists allow ingress from 0.0.0.0/0 or ::/0 to port 22/3389	45%
Boot volumes are not encrypted with Customer Managed Key (CMK)	96%
API keys are created for tenancy administrator users	25%
MFA is not enabled for all users with a console password	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 Vulnerabilities

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 legitimate access.

Take Action: Upgrade to OpenSSH 9.9p2 immediately to safeguard your infrastructure. Act fast—patch today! For a deep dive into these vulnerabilities and expert insights, visit our blog.

Stay protected by leveraging Qualys' comprehensive vulnerability detection and management. For more in-depth knowledge and details, visit Qualys ThreatPROTECT page and subscribe to receive the latest updates on threats and vulnerabilities.

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.

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 researchNewsletter@qualys.com. Until then, stay safe and secure!

Qualys.

Privacy Policy. Accessibility. Notice at Collection. Trust. Cookie Consent.