Qualys Threat Research Unit

APRIL 2025

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

8 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

3 Ubuntu bypasses uncovered by Qualys TRU

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

April's Must-Know Risks

Google Chrome Zero-day Vulnerability

CVE-2025-2783
QID: 382974, 382999

QVS 95

Windows CLFS elevation-of-privilege

CVE-2025-29824
QID: 92242, 92235, etc

QVS 95

Windows LDAP client RCE

CVE-2025-26663/CVE-2025-26670
QID: 92242, 92235, etc

QVS 95

Apache Tomcat RCE

CVE-2025-24813
QID: 732321, 732322, etc

QVS 95

Apple Backports Fixes for Three Zero-day Vulnerabilities

CVE-2025-24200-01, CVE-2025-24085
QID: 383013, 383014

QVS 95

tj-actions changed-files Supply Chain Vulnerability

CVE-2025-30066
QID: 383033

QVS 95

Fortinet FortiOS auth bypass (Node.js WebSocket)

CVE-2025-24472
QID: 44501

QVS 95

Ivanti Connect Secure / Policy Secure / ZTA

CVE-2025-22457
QID: 732234, 732410

QVS 92

CrushFTP Authentication Bypass Vulnerability

CVE-2025-31161
QID: 382978, 732399

QVS 92

Ingress NGINX critical Vulnerabilities

CVE-2025-24513-14, CVE-2025-1097-98, CVE-2025-1974
QID: 382971, 5003332, etc

QVS 75

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 TAM today to get yours.

Safeguarding Vulnerability Management Despite MITRE Funding Risks

Recent concerns over MITRE's funding outlook for CVEs raised questions about potential coverage gaps. While those uncertainties have been alleviated, Qualys moved swiftly to reinforce your protection. **Qualys, backed by 120+ white hat researchers and more than 25 threat intelligence feeds, builds detections directly from vendor advisories—not solely relying on MITRE. As a result, customers experience zero delay or degradation in signature quality**.

For more info, read our blog.

Cloud Security Snapshot: Key Misconfigurations

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
Usage of root account is not monitored	95%
MFA is not enabled for the root user account	41%
Network ACLs allow ingress from 0.0.0.0/0 to port 22	91%
EBS Volume is not encrypted by KMS using a customer managed Key (CMK)	77%
Access key 1 is not rotated every 90 days or less	87%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Storage accounts allow Blob public access	31%
Disk encryption on virtual machines is set to Off	40%
Keyvault are not recoverable	45%
Custom subscription Administrator Roles exist	46%
Expiration Date is not set for all Secrets in RBAC Key Vaults	65%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
KMS encryption keys are not rotated within a period of 90 days	67%
Logging is disabled for Cloud storage buckets	94%
API Keys are not rotated every 90 days	77%
Project has Service Account with Admin Privileges	26%
Pub/Sub topics are not encrypted using Customer-Managed Keys (CMKs)	96%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
IAM password policy does not meet minimum length of 14 or greater	98%
Object Storage Buckets are not encrypted with a Customer Managed Key CMK	60%
API keys are not rotated within 90 days or less	89%
Object Storage buckets are publicly visible	38%
Secret auto rotation is not enabled	95%

Note: Percentages reflect how many resources across all customers, have these misconfigurations.

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 TAM today to get your personalized report and secure your cloud**.

Qualys TRU Discovers Three Bypasses of Ubuntu Unprivileged User Namespace Restrictions

The Qualys Threat Research Unit (TRU) recently disclosed three security bypasses in Ubuntu's unprivileged user namespace restrictions. These bypasses each enable local attackers to create user namespaces with full administrative capabilities.

Leverage Qualys TruRisk Eliminate to Mitigate These Risks: To help organizations address these risks quickly, customers leveraging the Qualys agent can use the TruRisk Eliminate module. It allows the team to test and deploy the mitigation directly from the Qualys console, leveraging the Qualys agent. There is nothing new to install.

If you are not subscribed to the TruRisk Eliminate module, you can visit this page to start a trial or ask your TAM to enable a trial for you.

For a deep dive into these bypasses and expert insights, visit ours blog.

Stay protected by leveraging Qualys' comprehensive vulnerability detection and management.

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 April 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.