Qualys Threat Research Unit

JUNE 2025

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

6 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

2 LPE Flaws discovered by Qualys TRU

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

June's Must-Know Risks

Versa Concerto Authentication Bypass

CVE-2025-34027
QID: 530097, 732555

QVS 100

ConnectWise SC SQL Injection

CVE-2025-3935
QID: 383325, 530168

QVS 95

Google Chrome Zero-Day

CVE-2025-5419
QID: 383328

QVS 95

vBulletin RCE

CVE-2025-48827
QID: 732580, 530109

QVS 95

Apple Multiple Products

CVE-2025-43200
QID: 383360, 383359, 383358

QVS 95

MS WebDAV Remote Code Execution

CVE-2025-33053
QID: 92275, 92272

QVS 95

Invision Community RCE

CVE-2025-47916
QID: 732578, 530114

QVS 75

Veeam Backup and Replication

CVE-2025-23121
QID: 383390

QVS 75

Windows SMB Client EOP

CVE-2025-33073
QID: 92275, 92272

QVS 42

Windows Netlogon EoP

CVE-2025-33070
QID: 92275, 92272

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.

Qualys TRU Uncovers Chained LPE: SUSE 15 PAM to Full Root via libblockdev/udisks

The Qualys Threat Research Unit (TRU) has discovered two linked local privilege escalation (LPE) flaws.

The first (CVE-2025-6018) resides in the PAM configuration of openSUSE Leap 15 and SUSE Linux Enterprise 15. The second (CVE-2025-6019) affects libblockdev, is exploitable via the udisks daemon included by default on most Linux distributions and allows an "allow_active" user to gain full root privileges.

Given the ubiquity of udisks and the simplicity of the exploit, organizations must treat this as a critical, universal risk and deploy patches without delay.
For a deep dive into these vulnerabilities and expert insights, visit our Blog.

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 (%)
Ensure AWS Organizations changes are monitored	98.00%
Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 3389	96.00%
Ensure that DocumentDB Instances certificates are rotated	91.00%
Ensure IAM Database Authentication is Enabled for the DB Instances	90.00%
Ensure access keys unused for 90 days or greater are disabled	74.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure that Public Network Access is Disabled for storage accounts	90.00%
Ensure that Azure CosmosDB does not allow access from all networks	83.00%
Ensure that Storage Account Access Keys are Periodically Regenerated	86.00%
Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	66.00%
Disable RDP access on Network Security Groups from Internet	6.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure Private Google Access is enabled for all subnetwork in VPC Network	91.00%
Ensure that PostgreSQL instances are encrypted with CMKs	88.00%
Ensure API Keys are rotated every 90 days	80.00%
Ensure there are no unrestricted API keys available within your GCP project	72.00%
Ensure Project has no Service Account with Admin Privileges	28.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure boot volumes are encrypted with CMK	97.00%
Ensure user Customer Secret keys rotate within 90 days or less	98.00%
Ensure VM disks for critical VMs are encrypted with CSEK	95.00%
Ensure only to the tenancy administrator group has permissions on all resources	93.00%
Ensure MFA is enabled for all users with a console password	75.91%

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 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 May 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!