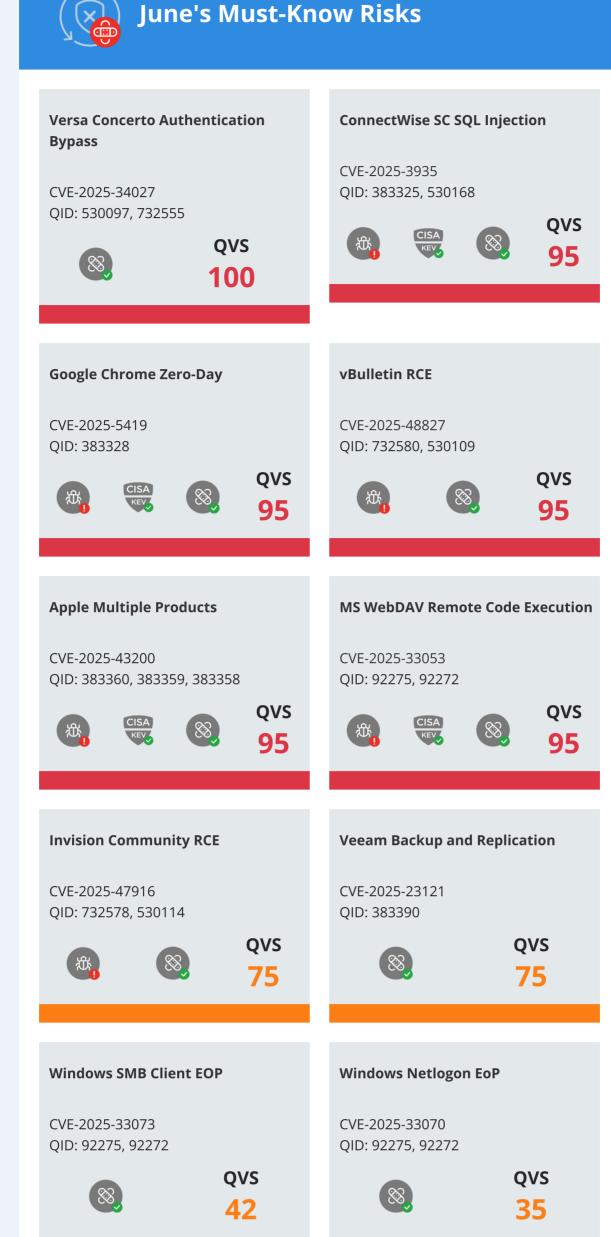




Measure, communicate, and eliminate your cyber risk—before it escalates into a crisis.



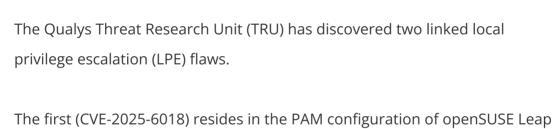
These vulnerabilities pose significant risks to your systems. To understand and address these critical threats, get your **personalized TruRisk Report**. Contact your Technical Account Manager today to get yours.

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

subscribe to receive the latest updates on threats and vulnerabilities.

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

libblockdev/udisks



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,

Misconfigurations

15 and SUSE Linux Enterprise 15. The second (CVE-2025-6019) affects

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 <u>Blog</u>.

Cloud Security Snapshot: Key

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

Resources

98.00%

96.00%

91.00%

Affected (%)



Ensure AWS Organizations changes are monitored

Ensure no Network ACLs allow ingress from

Ensure that DocumentDB Instances certificates

before it's too late.

0.0.0.0/0 to port 3389

are rotated

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 (%)

storage accounts	
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 (%)

Misconfiguration	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 98.00% days or less Ensure VM disks for critical VMs are encrypted with 95.00% **CSEK** Ensure only to the tenancy administrator group has 93.00% permissions on all resources **Ensure MFA is enabled for all users with a console** 75.91% password

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

misconfigurations.

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.

These misconfigurations pose significant risks to your cloud. To

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.

Accessibility. Notice at Collection. Trust. Cookie Consent.

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!