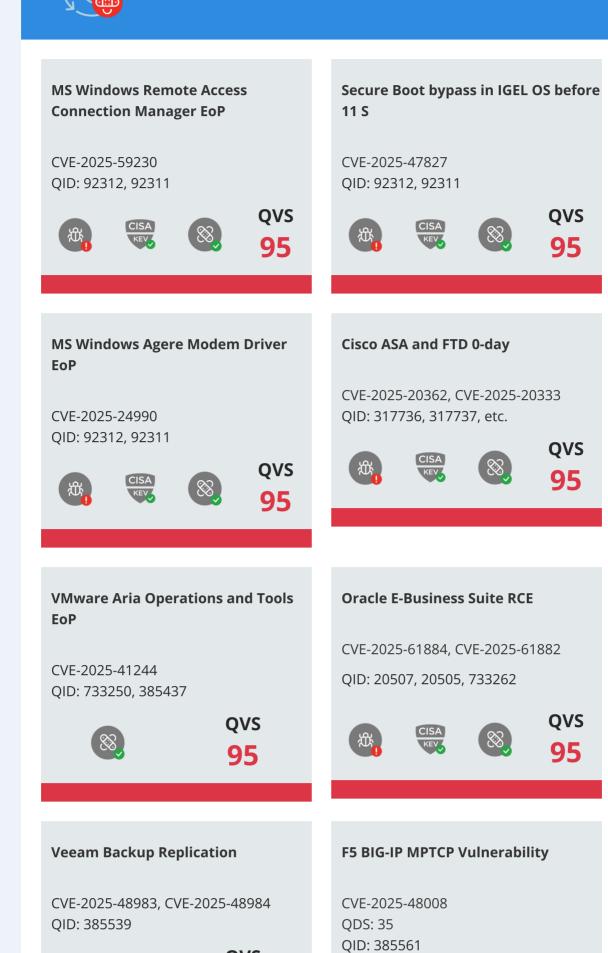




cyber risk—before it escalates into a crisis.

October's Must-Know Risks



These vulnerabilities pose significant risks to your systems. To understand and address these critical threats, get your personalized TruRisk Report.

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

subscribe to receive the latest updates on threats and vulnerabilities.

QVS

60

Cloud Security Snapshot: Key Misconfigurations

Contact your Technical Account Manager today to get yours.



Secrets should be auto rotated after not more

Network ACLs allow ingress from 0.0.0.0/0 or ::/0 to

No SQL Servers allow ingress from Internet (ANY

Expiration Date is set for all Secrets in Non RBAC

Private Endpoints are Used for Azure Key Vault

User customer Secret keys rotate within 90 days

Secure Boot is enabled on Compute Instance

Only one active API Key for any single OCI IAM

Autonomous Database is encrypted using

customer-managed key

before it's too late.

Misconfiguration

than 90 days

nort 3389/22

IP)

Key Vaults

or less

user

The following percentages reflect how many resources across all customers have these misconfigurations. **Amazon Web Services (AWS)**

Resources

98.00%

94.00%

52.00%

73.00%

69.00%

97.00%

94.00%

82.00%

21.00%

Affected (%)

port 3389/22		
File Storage Systems arenot encrypted with Customer Managed Keys (CMK)	88.00%	
Block public sharing setting is ON for the documents in all regions	87.00%	
Data stored in the Sagemaker Endpoint is securely encrypted at rest	97.00%	
Microsoft Azure		
Misconfiguration	Resources Affected (%)	
Storage accounts disallow Blob public access	25.00%	
Public Network Access is Disabled for storage accounts	88.00%	

Google Cloud Platform (GCP)		
Misconfiguration	Resources Affected (%)	
Cloud function is not anonymously or publicly accessible	14.00%	
BigQuery Table is encrypted with Customer- managed key	91.00%	
API Keys are rotated every 90 days	83.00%	
DNSSEC is enabled for Cloud DNS	53.00%	
No Cloud Run Service is Publicly Accessible	19.00%	
Oracle Cloud Infrastructure (OCI)		
Misconfiguration	Resources Affected (%)	

Network security groups allow ingress from 0.0.0.0/0 or ::/0 to port 3389	35.00%	
These misconfigurations pose significant risks to	your cloud. To	
understand and address these critical issues, get yo	our Cloud TruRisk	
Insight Report . This report identifies which misconfigurations are causing		
risks and provides actionable steps to remediate th	em. Contact your	
Technical Account Manager today to get your personalized report and		
secure your cloud.		
A Strategic Response to the Nation-State Breach	he F5 BIG-IP	

defense strategy to close the widening gap between attacker speed and defender response. Leveraging Qualys VMDR and asset inventory, organizations should immediately identify exposed BIG-IP instances, apply the 44-CVE patch set, harden management interfaces, and conduct continuous threat hunting. This incident highlights the critical need for real-time visibility and risk-based prioritization to stay ahead of sophisticated, state-sponsored threats.

Following the nation-state breach of F5 BIG-IP, Qualys emphasizes a proactive

accelerating against F5 BIG-IP while patching is slowing. With the new 44-CVE bundle (K000156572) closing windows revealed by stolen code, treat every item as high-urgency. Attackers now move in hours or days—especially with insider insight. See the charts and what to do next in the blog.

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

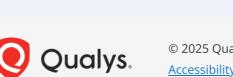
Our latest TRU analysis exposes a risk-velocity mismatch: attackers are

security posture. Don't wait—proactive steps now can prevent costly breaches later.

Thank you for being part of our October newsletter! We hope these insights empower you to enhance your security posture. Get ready for next month's edition, filled with

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!

the latest updates and expert threat research tips.



Accessibility. Notice at Collection. Trust. Cookie Consent.