Qualys Threat Research Unit

October 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

F5 BIG-IP 44-CVE bundle

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

October's Must-Know Risks

MS Windows Remote Access Connection Manager EoP

CVE-2025-59230
QID: 92312, 92311

QVS **95**

Secure Boot bypass in IGEL OS before 11 5

CVE-2025-47827
QID: 92312, 92311

QVS **95**

MS Windows Agere Modem Driver EoP

CVE-2025-24990
QID: 92312, 92311

QVS **95**

Cisco ASA and FTD 0-day

CVE-2025-20362, CVE-2025-20333
QID: 317736, 317737, etc.

QVS **95**

VMware Aria Operations and Tools EoP

CVE-2025-41244
QID: 733250, 385437

QVS **95**

Oracle E-Business Suite RCE

CVE-2025-61884, CVE-2025-61882
QID: 20507, 20505, 733262

QVS **95**

Veeam Backup Replication

CVE-2025-48983, CVE-2025-48984
QID: 385539

QVS **60**

F5 BIG-IP MPTCP Vulnerability

CVE-2025-48008
QDS: 35
QID: 385561

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.**

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.

The following percentages reflect how many resources across all customers have these misconfigurations.

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
Secrets should be auto rotated after not more than 90 days	98.00%
Network ACLs allow ingress from 0.0.0.0/0 or ::/0 to port 3389/22	94.00%
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%
No SQL Servers allow ingress from Internet (ANY IP)	52.00%
Expiration Date is set for all Secrets in Non RBAC Key Vaults	73.00%
Private Endpoints are Used for Azure Key Vault	69.00%

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 (%)
User customer Secret keys rotate within 90 days or less	97.00%
Secure Boot is enabled on Compute Instance	94.00%
Autonomous Database is encrypted using customer-managed key	82.00%
Only one active API Key for any single OCI IAM user	21.00%
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 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**.

A Strategic Response to the F5 BIG-IP Nation-State Breach

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

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