Qualys Threat Research Unit

January 2026

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

7 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

Cybersecurity Predictions for 2026

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

January's Must-Know Risks

Fortinet Authentication Bypass

CVE-2026-24858
QID: 530877, 44914, 44913

QVS 95

MS Office Security Feature Bypass

CVE-2026-21509
QID: 110516

QVS 95

SmarterTools Smartermail Authentication Bypass

CVE-2026-23760
QID: 733633

QVS 95

Cisco AsyncOS Secure Email Gateway RCE

CVE-2025-20393
QID: 733541, 317752

QVS 95

MongoDB Memory Disclosure (MongoBleed)

CVE-2025-14847
QID: 20525, 386257

QVS 95

Windows DWM Information Disclosure

CVE-2026-20805
QID: 92347

QVS 95

Zimbra LFI Vulnerability

CVE-2025-68645
QID: 530803, 386229

QVS 95

MS Office Remote Code Execution

CVE-2026-20952/20953
QID: 110515

QVS 35

Secure Boot Certificate Expiration Bypass

CVE-2026-21265
QID: 92342, 92341

QVS 30

Windows VBS Enclave Elevation of Privilege

CVE-2026-20876
QID: 92342, 92341

QVS 30

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.

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
Lambda function has Admin Privileges	25.00%
Redshift clusters publicly accessible	18.00%
Root account usage not monitored	95.00%
Network ACLs allow SSH from 0.0.0.0/0	91.00%
MFA not enabled for root user	56.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
No expiration date for secrets in Key Vaults	84.00%
SQL Servers allow ingress from ANY IP	55.00%
RDP access enabled from Internet	8.00%
App Service Authentication not configured	83.00%
Storage Accounts not using latest TLS	14.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Service account keys not rotated in 90 days	90.00%
Instances using default SA with full access	40.00%
Project-wide SSH keys not blocked for VMs	94.00%
Cloud function publicly accessible	9.00%
Service Account with Admin Privileges	31.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
File Storage not encrypted with CMK	84.00%
Secure Boot not enabled on Compute	95.00%
Security lists allow SSH from 0.0.0.0/0	58.00%
User API keys not rotated in 90 days	93.00%
Autonomous DB missing Mutual TLS auth	52.00%

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**.

Cybersecurity Predictions for 2026: The Maturation of Risk-First Models

By the end of 2025, most security leaders reached the same conclusion: We have the tools and the telemetry, but we need better execution. 2026 marks the shift from simply observing risk to actively governing it.

In our latest forecast, we explore seven key predictions for the year ahead, including:

- The Rise of the ROC: How Risk Operations Centers are operationalizing exposure management.
- AI as a Filter: Moving beyond the hype to use AI for reducing signal noise and prioritizing threats.
- Radical Transparency: Why real-time breach disclosure is becoming the ultimate trust-building control.
- Strategic Insurance: How cyber insurance is evolving from a checklist to a strategic risk-financing lever.

Read the Full 2026 Predictions Here

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 January 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.