



January 2026

This Month's Update

# Threat Research Newsletter

Stay informed to keep your systems secure and resilient

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

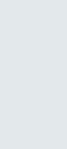
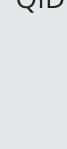
CVE-2026-24858  
QID: 530877, 44914, 44913



QVS  
95

### MS Office Security Feature Bypass

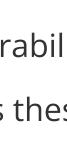
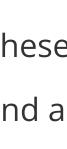
CVE-2026-21509  
QID: 110516



QVS  
95

### SmarterTools Smartermail Authentication Bypass

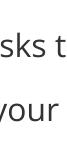
CVE-2026-23760  
QID: 733633



QVS  
95

### Cisco AsyncOS Secure Email Gateway RCE

CVE-2025-20393  
QID: 733541, 317752



QVS  
95

### MongoDB Memory Disclosure (MongoBleed)

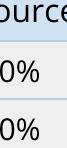
CVE-2025-14847  
QID: 20525, 386257



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

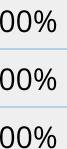
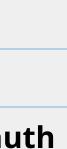
CVE-2026-21265  
QID: 92342, 92341



QVS  
30

### Windows VBS Enclave Elevation of Privilege

CVE-2026-20876  
QID: 92342, 92341

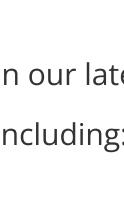


QVS  
30

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

### Microsoft Azure

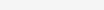
Misconfiguration	Resources Affected (%)
<b>No expiration date for secrets in Key Vaults</b>	84.00%
<b>SQL Servers allow ingress from ANY IP</b>	55.00%
<b>RDP access enabled from Internet</b>	8.00%
<b>App Service Authentication not configured</b>	83.00%
<b>Storage Accounts not using latest TLS</b>	14.00%

### Google Cloud Platform (GCP)

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

### Oracle Cloud Infrastructure (OCI)

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



## Cybersecurity Predictions for 2026: The Major Risk Evolution 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](#)

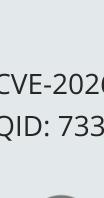


Stay protected by leveraging Qualys' comprehensive vulnerability detection and management.

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.



## Cybersecurity Predictions for 2026: The Major Risk Evolution Models



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.



© 2026 Qualys, Inc. All rights reserved. [Privacy Policy](#)

[Accessibility](#) [Data Collection](#) [Trust](#) [Consent](#)