Qualys Threat Research Unit

February 2026

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

10 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

Qualys TruConfirm: The End of Vulnerability Guesswork

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

February's Must-Know Risks

Cisco SD-WAN Auth Bypass Vulnerability

CVE-2026-20127
QID: 317761

QVS 95

Google Chrome Use-after-free Zero-day Vulnerability

CVE-2026-2441
QID: 386573

QVS 95

Apple iOS Zero-day Vulnerability

CVE-2026-20700
QID: 386542, 610759

QVS 95

BeyondTrust PRA RCE Vulnerability

CVE-2026-1731
QID: 733671

QVS 95

Windows Remote Desktop Services EoP Vulnerability

CVE-2026-21533
QID: 92350, 92351, 92361

QVS 95

Windows Shell Security Feature Bypass Vulnerability

CVE-2026-21510
QID: 92350, 92351, 92359

QVS 95

Microsoft Word Security Feature Bypass Vulnerability

CVE-2026-21514
QID: 110519

QVS 95

Windows Remote Access Connection Manager DoS Vulnerability

CVE-2026-21525
QID: 92350, 92351, 92360

QVS 95

MSHTML Framework Security Feature Bypass Vulnerability

CVE-2026-21513
QID: 92350, 92351, 92358

QVS 95

Desktop Windows Manager EoP Vulnerability

CVE-2026-21519
QID: 92350, 92351, 92357

QVS 95

For more in-depth information, visit the 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. Identify critical cybersecurity threats facing your organization and learn the strategies to mitigate them. Act fast—secure your cloud before it's too late.
The following percentages reflect the number of resources across all customers that have these misconfigurations.

Amazon Web Services (AWS)

Misconfiguration	Resources Affected (%)
Ensure no Network ACLs allow ingress from 0.0.0.0/0 or ::/0 to port 22	93.00%
Ensure multi-factor authentication is enabled for the root user account	58.00%
Ensure console credentials unused for 45 days or more are disabled	9.00%
Ensure no security groups allow inbound SSH (22) from 0.0.0.0/0 or ::/0	13.00%
Ensure AWS Security Hub is enabled in all regions	65.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Configure Microsoft Defender for Cloud to check VM OS updates	37.00%
Ensure expiration dates are set for all secrets in non-RBAC Key Vaults	88.00%
Block inbound SSH (port 22) from 0.0.0.0/0 or ::/0 in Network Security Groups	11.00%
Block inbound RDP (3389) from 0.0.0.0/0 or ::/0 in Network Security Groups	8.00%
Ensure Encryption at host is enabled for virtual machines	98.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure Block Project-wide SSH keys is enabled for VM instances	92.00%
Ensure API Keys are rotated at least every 90 days	82.00%
Ensure no service account has admin-level privileges	28.00%
Rotate user-managed service account keys every 90 days	91.00%
Require SSL/TLS for all Cloud SQL incoming connections	46.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure write level Object Storage logging is enabled for all buckets	97.00%
Ensure no Object Storage buckets are publicly visible	36.00%
Ensure Secure Boot is enabled on compute instances	96.00%
Restrict Oracle Functions apps using secure network controls	87.00%
Block security list ingress to SSH (22) from 0.0.0.0/0 or ::/0 to port 22	58.00%

These misconfigurations pose significant risks to your cloud. To understand and address these critical issues, **get your Cloud TruRisk Insight Report**. This report identifies the misconfigurations that pose risks and provides actionable steps to remediate them. **Contact your Technical Account Manager today to get your personalized report and secure your cloud**.

Qualys TruConfirm: The End of Vulnerability Guesswork

Qualys ETM introduces TruConfirm, an exploit-validation capability that goes beyond traditional version-based scanning by safely testing whether a vulnerability can be exploited in your live environment. It uses production-safe payloads, cryptographic verification, and out-of-band detection to deliver deterministic proof of exploitability—not just theoretical risk. This lets security teams cut through alert noise and focus remediation on the small subset of vulnerabilities that genuinely pose a threat.

Discover how TruConfirm replaces vulnerability guesswork with proof of exploitability. Learn more.

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 February 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.