

Sep 2026

This Month's Update

Threat Research Newsletter

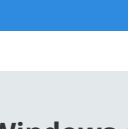
Stay informed to keep your systems secure and resilient

10 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

ROCon (Risk Operations Conference)
Americas: October 2026

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



September's Must-Know Risks

Windows ALPC EoP Vulnerability

CVE-2026-85880
QID:92455,92462



QVSS
9.5

SonicWall SMA1000 SSRF Vulnerability

CVE-2026-83548
QID:735393,388624



QVSS
9.5

Windows Update Stack EoP Vulnerability

CVE-2026-81963
QID:92453,92455



QVSS
9.5

Cisco Secure FMC Auth Bypass Vulnerability

CVE-2026-20079
QID:735397,317770



QVSS
9.5

Citrix NetScaler ADC/Gateway RCE Vulnerability

CVE-2026-88772
QID:388834



QVSS
9.5

GitLab CE/EE Unauth Arbitrary File Read Vulnerability

CVE-2026-85706
QID:735403



QVSS
9.5

Cisco Secure Email Gateway SQL Injection Vulnerability

CVE-2026-76461
QID:317880



QVSS
9.5

Cisco Identity Services Engine Auth Bypass Vulnerability

CVE-2026-76460
QID:317886



QVSS
9.5

F5 BIG-IP APM Heap-Based Buffer Overflow Vulnerability

CVE-2026-94127
QID:388803



QVSS
9.5

Citrix NetScaler ADC and Gateway Auth Bypass Vulnerability

CVE-2026-19490
QID:388454



QVSS
9.5

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 MFA is enabled for the root user account	64.00%
Ensure MFA delete is enabled on S3 buckets	98.00%
Ensure MFA is enabled for all IAM users that have a console password	62.00%
Ensure management console sign-in without MFA is monitored	98.00%
Ensure MFA is enabled in Directory Service	99.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure Azure Batch local authentication is disabled	97.00%
Ensure Service Fabric clusters use Azure AD authentication	31.00%
Ensure Data Access Authentication Mode is enabled for disks	98.00%
Ensure that Microsoft Entra authentication is configured for SQL Servers	17.00%
Ensure App Service Authentication is set on Web Apps	11.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure API Keys are rotated every 90 days	70.00%
Ensure every service account is configured solely with GCP-managed key	20.00%
Ensure Block Project-wide SSH keys enabled for VM instances	90.00%
Enforce 90-day rotation for user-managed/external service account keys	92.00%
Ensure no unrestricted API keys exist in the GCP project	71.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure MFA is enabled for all users with a console password	79.00%
Ensure Mutual TLS is required for Autonomous Databases	87.00%
Ensure OCI IAM credentials unused for 45 days or more are disabled	92.00%
Ensure API keys are not created for tenancy administrator users	19.00%
Enable Cloud Guard in the tenancy root compartment	29.00%

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.**



ROCon (Risk Operations Conference) Americas: October 2026

ROCon Americas 2026 will be held in Austin in October this year. The next evolution of QSC, where the brightest minds in cybersecurity unite to chart the future of proactive cyber risk management for the Frontier AI era. The event convenes cybersecurity leaders, CISOs, and practitioners around a single mission: moving security teams from reactive defense to proactive risk reduction. Sessions center on operationalizing risk-quantifying exposure, prioritizing remediation, and measurably strengthening organizational resilience.

Attendees explore how Risk Operations reframes vulnerability management, threat intelligence, and compliance as a unified, business-aligned discipline. Through keynotes, technical tracks, and peer exchange, ROCon equips teams to reduce material risk faster and communicate it clearly to leadership. It positions risk operations as the connective tissue between security telemetry and executive decision-making.

Read our blog [here](#).



Qualys.



ROCon 26

The Risk Operations Conference

AMERICAS

See What's Next in AI-Speed Risk Operations

October 13-15 | Austin, TX

Register Now



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 September 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.

© 2026 Qualys, Inc. All rights reserved. [Privacy Policy](#). [Accessibility](#). [Notice at Collection](#). [Trust](#). [Cookie Consent](#).