Qualys Threat Research Unit

Aug 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

Agent Insta: Closing the Detection Gap in Exposure Management

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

August's Must-Know Risks

Broadcom VMware vCenter Path Traversal Vulnerability

CVE-2026-59310
QID:216357,216356

QVSS 10

Cisco Secure Firewall ASA/FTD DoS Vulnerability

CVE-2026-20349
QID:317873,317874

QVSS 9.5

IBM Langflow RCE Vulnerability

CVE-2026-9198
QID:734865

QVSS 9.5

Progress Kemp LoadMaster Pre-Auth RCE Vulnerability

CVE-2026-8037
QID:734601

QVSS 9.5

JetBrains TeamCity Remote Code Execution Vulnerability

CVE-2026-63077
QID:388160

QVSS 9.5

Fortinet FortiSandbox OS Command Injection Vulnerability

CVE-2026-25089
QID:734396

QVSS 9.5

Windows Ancillary Function Driver for WinSock EoP Vulnerability

CVE-2026-68820
QID:92439,92440

QVSS 9.5

Microsoft Exchange Server EoP Vulnerability

CVE-2026-62911
QID:50149

QVSS 4.2

Windows AD CS RCE Vulnerability

CVE-2026-62818
QID:92439,92440

QVSS 3.5

Microsoft SharePoint Server RCE Vulnerability

CVE-2026-65665
QID:110531

QVSS 3.5

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 that custom IAM Password Policy is Defined	26.00%
Ensure MFA is enabled for the root user account	64.00%
Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	88.00%
Ensure management console sign-in without MFA is monitored	97.00%
Ensure AWS ElastiCache Redis clusters are encrypted at rest using a CMK	61.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure that Blob Storage is configured with Diagnostic Settings	73.00%
Ensure that File Storage is configured with Diagnostic Settings	75.00%
Ensure that Queue Storage is configured with Diagnostic Settings	79.00%
Ensure that diagnostic settings for Azure KeyVault is set to ON	97.00%
Ensure Diagnostic Setting captures appropriate categories	42.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure Cloud SQL MySQL instances require SSL for all connections	77.00%
Set Cloud SQL MySQL local_infile flag to OFF	87.00%
Ensure Cloud SQL MySQL instances do not have public IPs	23.00%
Require all incoming Cloud SQL for SQL Server connections to use SSL	48.00%
Ensure Cloud SQL Server's contained database authentication is set to Off	64.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure Autonomous Database requires Mutual TLS (mTLS) authentication	58.00%
Ensure Autonomous Database is encrypted with a customer-managed key	76.00%
Ensure DB systems' NSGs restrict database access	90.00%
Ensure DB System databases are encrypted using a customer-managed key	99.00%
Ensure Autonomous Database does not allow secure access from everywhere	51.00%

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**.

Agent Insta: Closing the Detection Gap in Exposure Management

Frontier AI has cut CVE weaponization time from days to hours, but scan-based detection still lags 24–36 hours behind disclosure, leaving critical exposure windows unmonitored. Qualys closes this gap with **InstaScan**, powered by its new Agent Insta engine, the industry's first scanless detection capability. It continuously correlates newly published advisories against existing asset inventory and telemetry from Qualys and third-party tools, flagging exposed assets within minutes of disclosure, with no new scan jobs required.

InstaScan achieves 90%+ detection coverage across technologies representing 60–70% of enterprise vulnerability volume, feeding cleaner, faster signals into TruRisk prioritization and Agent Vai's validation and remediation workflows, closing the loop from disclosure to fix without third-party stitching or reliance on stale data. InstaScan will be available on the Qualys ETM platform by the end of August 2026.

Read our blog 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.

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 August 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.