Qualys Threat Research Unit

December 2025

This Month's Update

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

8 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

React2Shell: React Server Components Remote Code Execution Vulnerability

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

December's Must-Know Risks

React Server Components (React2Shell)

CVE-2025-55182
QID: 733480, 48336

QVS 100

Google Chrome Zero-day

CVE-2025-14174
QID: 386201

QVS 95

GeoServer Unauthenticated XML XXE

CVE-2025-58360
QID: 733470

QVS 95

Apple iOS Zero-day

CVE-2025-43529
QID: 610752, 610753, 386207, 386205

QVS 95

Windows Cloud Files Mini Filter Driver Elevation of Privilege

CVE-2025-62221
QID: 92339, 92336

QVS 95

Cisco AsyncOS Secure Email Gateway and Web Manager RCE

CVE-2025-20393
QID: 317752, 733541

QVS 95

Fortinet Zero-day Authentication Bypass

CVE-2025-59718
QID: 44861, 44862

QVS 72

React Server Components Denial of Service

CVE-2025-55184
QID: 733519

QVS 42

Ivanti EPM Arbitrary Code Exec

CVE-2025-10573
QID: 386197

QVS 37

PowerShell Remote Code Execution

CVE-2025-54100
QID: 92339, 92336

QVS 35

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. 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 multi-factor authentication is enabled for all IAM users that have a console password	57.00%
Ensure the default security group of every Virtual Private Cloud restricts all traffic	89.00%
Ensure Lambda environment variables are encrypted at-rest with Customer Managed Key	75.00%
Ensure IAM Database Authentication is Enabled for the Database Cluster	82.00%
Ensure Relational Database Service PostgreSQL Cluster enforces encrypted connections only	59.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure no SQL Servers allow ingress from Internet (ANY IP)	53.00%
Ensure keyvault is recoverable	44.00%
Ensure that Unattached disks are encrypted with Customer Managed Key	94.00%
Ensure that all disk snapshots are encrypted with Customer-managed key	82.00%
Ensure App Service Authentication is set on Function Apps	84.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure critical VM disks are encrypted with customer-supplied keys	95.00%
Ensure Block Project-wide SSH keys enabled for VM instances	92.00%
Instances should not use the default service account with full Cloud API access	51.00%
Ensure that BigQuery Dataset is encrypted with Customer-managed key	91.00%
Ensure user-managed/external keys for service accounts are rotated every 90 days or less	91.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure Object Storage Buckets are encrypted with a Customer Managed Key	61.00%
Ensure user API keys rotate within 90 days or less	92.00%
Ensure Block Volumes are encrypted with Customer Managed Keys	78.00%
Ensure secret auto rotation should be enabled	96.00%
Ensure user Auth Tokens rotate within 90 days or less	97.00%

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**.

React2Shell: React Server Components (RSC) Remote Code Execution Vulnerability

A critical RCE flaw called React2Shell was disclosed on December 3, 2025, tracked as CVE-2025-55182 with CVSS 10.0. It affects React Server Components (RSC) in React 19.0.0–19.2.0 and frameworks like Next.js 15.x and 16.x using the RSC Flight protocol. The vulnerability results from unvalidated deserialization of Flight payloads, enabling attackers to inject arbitrary objects for remote code execution.

After disclosure, threat actors swiftly targeted internet-facing Next.js/RSC apps, exploiting the issue for environment discovery, command beaconing, reverse shells, cryptomining (XMRig), and backdoors like Sliver. Multiple groups linked to China and others have used React2Shell, risking data theft, persistent compromise, and operational disruption.

For more details, read our blog.

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 December 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.