Qualys Threat Research Unit

April 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

Mythos Inflection Point: Navigating the Vulnerability Disclosure Avalanche & Shrinking Exploitation Window

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

April's Must-Know Risks

Cisco Secure FMC RCE Vulnerability
CVE-2026-20131
QID: 317769
QVS 100

Google Chrome Zero-day Vulnerability
CVE-2026-5281
QID: 386954
QVS 95

Ivanti EPMM RCE Vulnerability
CVE-2026-1340
QID: 733655
QVS 95

F5 BIG-IP APM RCE Vulnerability
CVE-2026-53521
QID: 385564
QVS 95

FortiClient EMS SQL Injection Vulnerability
CVE-2026-21643
QID: 386518
QVS 95

Langflow Remote Code Injection Vulnerability
CVE-2026-33017
QID: 733892
QVS 95

Microsoft SharePoint Server Spoofing Vulnerability
CVE-2026-32201
QID: 110523
QVS 95

FortiClientEMS Improper Access Control Vulnerability
CVE-2026-35616
QID: 386970
QVS 95

Adobe Acrobat & Reader Arbitrary Code Execution Vulnerability
CVE-2026-34621
QID: 387005
QVS 95

Microsoft Defender Elevation of Privilege Vulnerability
CVE-2026-33825
QID: 92373
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.**

The Physics Gap: When Defenders Lose the Race Before It Starts

Qualys Threat Research Unit mapped 52 high-profile weaponized CVEs against two timelines — how fast attackers exploited them vs. how fast the average organization remediated them.

88% were remediated slower than they were exploited. Half were weaponized before public disclosure.

Each dot is a real vulnerability. The diagonal is parity. Everything above the line is a loss — and for the class of CVEs that define enterprise risk, losing is now the norm.

See the full data and what actually closes the gap in The Broken Physics of Remediation. **Read the report**

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 (%)
Enforce encrypted connections for RDS SQL instances	85.00%
Ensure Classic Elastic Load Balancer does not use unencrypted protocols	82.00%
Encrypt DynamoDB tables using KMS Customer Managed Key	47.00%
Encrypt AppFlow flows using Customer Managed Key	84.00%
Encrypt ML storage volumes for Hyperparameter Tuning Jobs using Customer Managed Key	72.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Use AES-256-GCM or higher for SMB channel encryption	99.00%
Enable customer-managed key encryption for Cognitive Services	97.00%
Enable encryption at host for Virtual Machine Scale Sets	95.00%
Use Customer Managed Keys for Event Hub namespace encryption	97.00%
Use a Customer Managed Keys for SQL Server TDE protector	89.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Encrypt critical VM disks using Customer-Supplied Encryption Keys	95.00%
Rotate KMS keys every 90 days	36.00%
Enable Customer-Managed Encryption Keys for boot disks	92.00%
Enable application-layer secret encryption for the Kubernetes cluster	81.00%
Rotate KMS encryption keys every 90 days	47.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Encrypt boot volumes with Customer Managed Key	94.00%
Encrypt object storage buckets using Customer Managed Key	62.00%
Encrypt block volumes using Customer Managed Key	71.00%
Encrypt block volume backups using Customer Managed Key	94.00%
Encrypt Kubernetes secrets at rest in etcd	98.00%

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**.

Mythos Inflection Point: Navigating the Vulnerability Disclosure Avalanche & Shrinking Exploitation Window

The Qualys blog post describes the Mythos Inflection Point, where AI models like Anthropic's Project Glasswing autonomously discover and exploit vulnerabilities, triggering a surge in disclosures. At the same time, shrinking exploitation windows to hours—or even before patches exist.

Vulnerability volume overwhelms teams already backlogged, as Google M-Trends 2026 data shows exploitation starting pre-disclosure ("minus seven days"). Traditional CVSS prioritization ignores real-world controls like WAFs, where <1% of theoretical risks are found to be exploitable in production. Prioritize by business context, internet exposure, and validated exploitability using attacker's eye view techniques for confirmation.

For more information, please read our blog for more information.

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 April 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.