Qualys Threat Research Unit

March 2026

This Month's Update

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

11 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

CrackArmor: Critical AppArmor Flaws Enable Local Privilege Escalation

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

TRU Research Report: The Broken Physics of Remediation

For years, security teams assumed they could outrun attackers—reduce MTTR, patch faster, and stay ahead. That model no longer holds.
In our latest Qualys Threat Research Unit report, The Broken Physics of Remediation, we analyzed 18+ CISA KEV records across 10,000 organizations.

The findings are clear:
✅ Critical vulnerability volume is up 6.6x, while exposure windows continue to grow.
✅ Organizational attack surfaces have expanded faster than teams can absorb
✅ Time-to-Exploit is now negative — vulnerabilities are weaponized before patches exist

The problem is not speed; it is the operational model itself.
Any architecture that depends on human-speed response carries structural risk. The shift to autonomous defense through a Risk Operations Center is no longer optional.
Read the report

March's Must-Know Risks

Cisco FMC Remote Code Execution Vulnerability

CVE-2026-20131
QID: 377769

QVS 100

BeyondTrust OS Command Injection Vulnerability

CVE-2026-1731
QID: 733834,733671

QVS 100

Ivanti EPM Authentication Bypass Vulnerability

CVE-2026-1603
QID: 386530

QVS 95

VMware Aria Command Injection Vulnerability

CVE-2026-22719
QID: 733801

QVS 95

Google Chrome Zero-day vulnerabilities

CVE-2026-3909,3910
QID: 386790,386791

QVS 95

Cisco Catalyst SD-WAN Auth Bypass Vulnerability

CVE-2026-20127
QID: 317761

QVS 95

SQL Server EoP Vulnerability

CVE-2026-21262
QID: 386758

QVS 35

.NET Denial of Service Vulnerability

CVE-2026-26127
QID: 92366

QVS 35

Windows Print Spooler RCE Vulnerability

CVE- 2026-23669
QID: 92365,92364

QVS 35

Microsoft Excel Information Disclosure Vulnerability

CVE-2026-26144
QID: 110521

QVS 30

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.

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.

CrackArmor: Critical AppArmor Flaws Enable Local Privilege Escalation

Qualys researchers discovered nine critical vulnerabilities in AppArmor (named "CrackArmor"). AppArmor is a Linux kernel security module that provides mandatory access control in distributions such as Ubuntu, Debian, and SUSE. These flaws have been present since kernel version 4.11 in 2017. Successful exploitation of the flaws may allow unprivileged local users to bypass protections, escalate to root, trigger kernel panics to cause denial-of-service, and break container isolation.

An attacker may exploit the vulnerability by leveraging the interaction between standard system tools such as su and sudo.
The vulnerability originates from "confused deputy" flaws that enable profile manipulation via pseudo-files such as /sys/kernel/security/apparmor/.load, leading to policy bypasses, stack exhaustion, and exploits involving tools such as Sudo and Postfix. Attackers can load "deny-all" profiles to block services, trigger recursive stack overflows to trigger reboots, or exploit use-after-free bugs to escalate to kernel space.

For more information, please read our blog.

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 (%)
Enable key rotation reminders for all Storage Accounts	95.00%
Disable public network access for storage accounts	88.00%
Enable 'Default to Microsoft Entra authorization' in Azure portal	89.00%
Enable versioning on Azure Blob Storage accounts	94.00%
Set Storage Accounts' default network rule to deny	66.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Enable key rotation reminders for all Storage Accounts	95.00%
Disable public network access for storage accounts	88.00%
Enable 'Default to Microsoft Entra authorization' in Azure portal	89.00%
Enable versioning on Azure Blob Storage accounts	94.00%
Set Storage Accounts' default network rule to deny	66.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Enforce separation of duties when assigning service account roles	08.00%
Use only GCP-managed keys for service accounts	20.00%
Avoid project-level roles enabling service account impersonation/management	98.00%
Rotate KMS keys every 90 days	45.00%
Avoid default service account with full Cloud API access on instances	41.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Ensure that DocumentDB Instances certificates are rotated	97.00%
Ensure DocumentDB Cluster is not listening on default port	83.00%
Set DocumentDB backup retention to at least 7 days	44.00%
Enable audit logs export to CloudWatch for DocumentDB	49.00%
Ensure DocDB TLS is not disabled	14.00%

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**.

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 March 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.