Qualys Threat Research Unit

July 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

RefluXFS: A Linux Kernel Local Privilege Escalation to Root in XFS (CVE-2026-64600)

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

RefluXFS: A Linux Kernel Local Privilege Escalation to Root in XFS (CVE-2026-64600)

Qualys Threat Research Unit (TRU) discovered RefluXFS, a race condition in the Linux kernel's XFS filesystem copy-on-write path. Any ordinary local user account can trigger the flaw to overwrite protected files on disk and gain full root privileges - even on systems running SELinux in Enforcing mode. The bug has existed since kernel 4.11 (2017) and, by Qualys's own asset-inventory analysis, potentially affects over 16.4 million systems worldwide, including default installations of RHEL, Oracle Linux, Amazon Linux, and Fedora. Qualys recommends prioritizing patching for exposed and multi-tenant systems now that vendor-fixed kernels are available.

This discovery emerged from a structured research initiative between Qualys and Anthropic, where we integrated Claude Mythos Preview into our manual audit workflow to accelerate our research while maintaining strict human oversight.

For more information, please read our blog.

July's Must-Know Risks

Oracle E-Business Suite Improper Privilege Management Vulnerability

CVE-2026- 46817
QID:20580

QVSS **10**

Microsoft SharePoint Server Elevation of Privilege Vulnerability

CVE-2026- 56164
QID:110529

QVSS **9.5**

Splunk Enterprise Arbitrary File Creation Vulnerability

CVE-2026- 20253
QID:387594

QVSS **9.5**

Active Directory Federation Services EoP Vulnerability

CVE-2026-56155
QID:92417,92418

QVSS **9.5**

Adobe ColdFusion Arbitrary Code Execution Vulnerability

CVE-2026-48282
QID:387758

QVSS **9.5**

WordPress wp2shell REST API Batch-Routing Vulnerability

CVE-2026-63030
QID:734739

QVSS **9.5**

WordPress wp2shell Facilitated SQL Injection Vulnerability

CVE-2026-60137
QID:734738

QVSS **9.5**

Microsoft SharePoint Insecure Deserialization Vulnerability

CVE-2026-50522
QID:531809

QVSS **9.5**

Cisco Unified Communications Manager SSRF Vulnerability

CVE-2026-20230
QID:317856

QVSS **9.5**

Microsoft SharePoint Security Feature Bypass Vulnerability

CVE-2026-55040
QID:110529

QVSS **6.5**

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.**

CVE-2026-8933: snap-confine Set-Capabilities Flaw Enables Local Privilege Escalation

Qualys TRU discovered CVE-2026-8933, a high-severity local privilege escalation in snap-confine that allows an unprivileged local user to gain full root access on default installations of Ubuntu Desktop 24.04, 25.10, and 26.04. The snap-confine is the enforcement component that builds the execution environment for snap applications.

The exploit leverages two concurrent race conditions. First, the attacker mounts a FUSE filesystem on the temporary scratch directory immediately after creation, bypassing the mount namespace isolation snap-confine applies later and keeping the directory accessible outside the sandbox. Second, the attacker plants a symlink pointing to an arbitrary target, so snap-confine's open() call follows it and writes to that target, while a second race widens file permissions to 0666 before snap-confine calls fchown() to hand ownership to root.

Read our report here.

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 (%)
Monitor root account activity	96.00%
Monitor Virtual Private Cloud (VPC) Changes	96.00%
Ensure organization-level trail is configured	48.00%
Ensure S3 data event logging is enabled	75.00%
Monitor changes to AWS Organizations	98.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Use CMK encryption for the activity logs storage account	94.00%
Enable private links for Azure Event Grid topics	90.00%
Ensure Azure Event Grid domains have public access disabled	99.00%
Disable public network access for Azure Event Grid domains	83.00%
Disable local authentication for Azure Event Grid partner namespaces	44.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Ensure Cloud Audit Logging is enabled for all services and users	13.00%
Ensure log alerts for project ownership changes	96.00%
Ensure alerts for custom role changes	96.00%
Enable logging for Cloud Storage buckets	94.00%
Enable Cloud DNS logging on all VPC networks	67.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Enable write logging for all Object Storage buckets	97.00%
Ensure Event Rule monitors security list changes	93.00%
Ensure Data Flow application logging is enabled	99.00%
Ensure monitoring alert subscriptions are configured	37.00%
Ensure Cloud Guard is enabled in the root compartment	30.00%

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.

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 July 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.