Qualys Threat Research Unit

May 2026

Threat Research Newsletter

Stay informed to keep your systems secure and resilient

This Month's Update

12 Vulnerabilities exploited in the wild

20 Cloud misconfiguration risk exposure

CVE-2026-46333: Linux Kernel Local Root Privilege Escalation Vulnerability

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

May's Must-Know Risks

Linux Kernel CopyFail Resource Transfer Vulnerability

CVE-2026-31431
QID:387198

QVSS 9.5

cPanel/WHM CRLF Injection Auth Bypass Vulnerability

CVE-2026-41940
QID:734113,734114

QVSS 10

Ivanti EPMM Input Validation Vulnerability

CVE-2026-6973
QID:734188

QVSS 9.5

PAN-OS Out-of-bounds Write Vulnerability

CVE-2026-0300
QID:734142

QVSS 9.5

Cisco SD-WAN Controller Auth Bypass Vulnerability

CVE-2026-20182
QID:317854

QVSS 9.5

BerriAI LiteLLM SQL Injection Vulnerability

CVE-2026-42208
QID:734105

QVSS 9.5

Microsoft Exchange Server Spoofing Vulnerability

CVE-2026-42897
QID:50146

QVSS 9.5

Microsoft Windows Protection Mechanism Failure Vulnerability

CVE-2026-32202
QID:92370,92369

QVSS 9.5

Microsoft Defender Denial-of-Service Vulnerability

CVE-2026-45498
QID:92401

QVSS 9.5

Microsoft Defender Link Following Vulnerability

CVE-2026-41091
QID:387448

QVSS 9.5

Drupal Core SQL Injection Vulnerability

CVE-2026-9082
QID:734308

QVSS 9.5

Windows Netlogon RCE Vulnerability

CVE-2026-41089
QID:92386

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-2026-46333: Linux Kernel Local Root Privilege Escalation Vulnerability

The Qualys Threat Research Unit (TRU) has discovered a critical local privilege escalation and credential disclosure vulnerability in the Linux kernel. CVE-2026-46333 is a vulnerability in the Linux kernel's __ptrace_may_access() function. Successful exploitation of the vulnerability may allow an unprivileged local user to disclose sensitive files and execute arbitrary commands as root on default installations of several major distributions.

The vulnerability has existed since the release of Linux kernel v4.10 in 2016. Qualys warns that public exploits are already circulating and urges administrators to apply vendor patches immediately, rotate exposed credentials, and, optionally, harden systems by setting kernel.yama.ptrace_scope=2.

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 (%)
Block 0.0.0.0/0 and ::/0 ingress to port 22 in security groups	96.00%
Block Network ACL ingress from 0.0.0.0/0 or ::/0 on port 22	93.00%
Block NACL ingress from 0.0.0.0/0 or ::/0 to port 3389	94.00%
Ensure Amazon EKS public endpoint is not accessible from 0.0.0.0/0 or ::/0	42.00%
Monitor Network Access Control List (NACL) changes	14.00%

Microsoft Azure

Misconfiguration	Resources Affected (%)
Ensure Cloud Run services are not publicly accessible	08.00%
Disable internet SSH access on NSGs (ANY IP)	10.00%
Ensure Azure Virtual Network subnets use a Network Security Group	57.00%
Enable NSG flow logs to Log Analytics	35.00%
Ensure NSG Flow Log retention exceeds 90 days	92.00%

Google Cloud Platform (GCP)

Misconfiguration	Resources Affected (%)
Restrict SSH access from the internet	6.00%
Restrict RDP access from the internet	4.00%
Ensure network policy is enabled on Kubernetes Engine clusters	29.00%
Ensure Cloud Functions are not publicly accessible	13.00%
Ensure Cloud Run services are not publicly accessible	15.00%

Oracle Cloud Infrastructure (OCI)

Misconfiguration	Resources Affected (%)
Block NSG ingress from 0.0.0.0/0 or ::/0 on port 22	42.00%
Block NSG ingress from 0.0.0.0/0 and ::/0 to port 3389	39.00%
Block ingress to port 22 from 0.0.0.0/0 and ::/0 in security lists	58.00%
Block ingress from 0.0.0.0/0 and ::/0 to port 3389 in security lists	33.00%
Ensure default VCN security lists allow only ICMP traffic and block all other traffic	92.00%

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**.

Verizon 2026 DBIR: Key Insights on Vulnerability Remediation

The Verizon 2025 Data Breach Investigations Report has been published, and Qualys has served as a research partner and contributor. The report analyzes more than one billion remediation records tied to CISA's Known Exploited Vulnerabilities (KEV) catalog and highlights a growing gap between vulnerability discovery and remediation. The report highlights a growing gap between vulnerability discovery and remediation. Vulnerability exploitation accounted for 20% of breaches — a 34% year-over-year increase — while credential abuse remained the leading entry point at 22%, signaling that exploitation is rapidly closing the gap.

The report also warns that AI is accelerating the pace of attacks — reducing the time from disclosure to active exploitation — while remediation timelines remain measured in weeks or months. Researchers conclude that traditional, human-driven patch management is no longer sufficient, urging organizations to adopt automated, risk-based remediation and continuous validation strategies.

Read our full report: 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 May 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 research1Newsletter@qualys.com. Until then, stay safe and secure!

Qualys.