INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-20 18:51 UTC

Quest KACE Systems Management Appliance (SMA) - Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0055
Type	CVE Vulnerability
CVE ID	CVE-2025-32975
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0054 (68th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-05-04)
Affected Products	Quest KACE Systems Management Appliance (SMA)
Published	2026-04-20
Discovery Source	Cisa Kev

Executive Summary

A critical authentication bypass vulnerability (CVE-2025-32975, CVSS 9.8) in Quest KACE Systems Management Appliance allows unauthenticated attackers to impersonate legitimate users without credentials. KACE SMA is widely deployed in enterprise environments for endpoint management, patch deployment, and software distribution, meaning a successful attacker gains privileged access to the systems management infrastructure. CISA has confirmed active exploitation in the wild and set a remediation deadline of May 4, 2026, making immediate patching mandatory.

Technical Analysis

CVE-2025-32975 is an improper authentication vulnerability (CWE-287) in Quest KACE Systems Management Appliance. CVSS base score is 9.8. The flaw enables unauthenticated remote attackers to impersonate authenticated users without valid credentials, mapping to MITRE ATT&CK techniques T1078 (Valid Accounts), T1556 (Modify Authentication Process), and T1190 (Exploit Public-Facing Application). Quest's advisory KB4379499 addresses this CVE alongside three related vulnerabilities: CVE-2025-32976, CVE-2025-32977, and CVE-2025-32978, indicating a broader attack surface on the KACE SMA platform. The vulnerability is

confirmed in CISA's Known Exploited Vulnerabilities catalog. Specific affected version ranges and patch availability are documented in Quest advisory KB4379499 (https://support.quest.com/kb/4379499). No public proof-of-concept details are included here, as the vulnerability is actively exploited.

Action Checklist

1. Step 1: Containment, Restrict network access to the KACE SMA management interface immediately. Block unauthenticated external access at the firewall or network boundary. If the appliance is internet-facing, take it offline or isolate it to a management VLAN until patched. Reference Quest advisory KB4379499 for appliance-specific isolation guidance.
2. Step 2: Detection, Review KACE SMA authentication logs for sessions with anomalous user-agent strings, unexpected source IPs, or authentication events lacking corresponding credential validation. Correlate with Active Directory or identity provider logs for accounts showing KACE activity that does not match normal login patterns. Check for new or modified scheduled tasks, scripts, or software distribution packages created through the SMA console by unfamiliar sessions.
3. Step 3: Eradication, Apply the patch documented in Quest advisory KB4379499. Confirm the installed KACE SMA version meets or exceeds the remediated version specified in that advisory. Address all four CVEs (CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978) simultaneously, as Quest has bundled the fixes.
4. Step 4: Recovery, After patching, rotate credentials for all KACE SMA administrator and service accounts. Audit active sessions and revoke any sessions created during the exposure window. Review recently deployed packages, scripts, or policy changes executed through KACE SMA for unauthorized modifications. Confirm KACE SMA authentication logs show only expected login activity post-patch.
5. Step 5: Post-Incident, Audit KACE SMA placement in the network architecture. Management appliances with privileged endpoint access should never be internet-facing without strong authentication controls. Evaluate whether multi-factor authentication is enforced for KACE SMA access. Add KACE SMA authentication anomalies to SIEM detection rules. Review the three related CVEs (CVE-2025-32976 through CVE-2025-32978) to identify any additional control gaps exposed by this advisory.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal, and executive stakeholders immediately if any evidence of unauthorized software deployment, script execution, or policy modification is found in KACE SMA audit logs during the exposure window, as KACE SMA's role as an endpoint management platform means a single compromised session could have pushed malicious packages to hundreds or thousands of managed endpoints — triggering potential breach notification obligations under GDPR, HIPAA, or applicable state law.

Recovery Notes	After patching and credential rotation, maintain enhanced monitoring of KACE SMA authentication logs and managed endpoint telemetry for a minimum of 30 days, specifically watching for re-exploitation attempts, lateral movement from endpoints that received packages during the exposure window, and any scheduled tasks or scripts on managed endpoints that do not match the authorized software baseline. Rebuild the KACE SMA authorized software catalog baseline from a known-good export taken before the exposure window, and re-validate all software distribution packages currently queued or recently deployed against that baseline using file hashes. If any managed endpoint shows indicators of unauthorized package installation or anomalous process execution traceable to the KACE agent service, treat that endpoint as potentially compromised and initiate a separate endpoint IR workflow.
Forensic Artifacts	KACE SMA web server access logs (typically /var/log/kace/ or /data/www/logs/access.log) — CVE-2025-32975 authentication bypass sessions will appear as HTTP 200 responses to authentication endpoints (e.g., /ams/ or /adminui/) from unexpected source IPs with non-standard or absent KACE agent user-agent strings, and critically without a preceding credential POST in the same session flow | KACE SMA admin console audit trail (Admin > Logs > Audit) — post-exploitation activity will manifest as software distribution package creations, script additions, or policy modifications attributed to session IDs that do not correspond to known administrator accounts or that originated from anomalous source IPs during the exposure window | Active Directory Security Event Log Event IDs 4624 (successful logon), 4672 (special privileges assigned), 4768/4769 (Kerberos TGT/service ticket requests) for the KACE SMA service account — an attacker impersonating a KACE admin via CVE-2025-32975 may trigger AD authentication events from source IPs inconsistent with the appliance's known IP address | Windows Security Event Log Event ID 4688 (Process Creation) and Event ID 11707 (Windows Installer product installed) on KACE-managed endpoints — filter on processes or installations where the parent process is the KACE agent (KSMAAgent.exe or equivalent) and timestamps fall within the exploitation exposure window, indicating potential malicious payload delivery via the compromised SMA console | Pre-isolation full PCAP of KACE SMA management interface traffic — network-level evidence will show the absence of a valid credential exchange in the HTTP/HTTPS session handshake for bypassed sessions, and may reveal attacker C2 callback traffic or data exfiltration initiated from the appliance following successful impersonation

Per-Action IR Details

Step 1: Containment — Restrict network access to the KACE SMA management interface immediately. Block unauthenticated external access at the firewall or network boundary. If the appliance is internet-facing, take it offline or isolate it to a management VLAN until patched. Reference Quest advisory KB4379499 for appliance-specific isolation guidance.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 (Establish and Maintain a Secure Network Architecture) — restrict KACE SMA management port (default TCP 443/80) to dedicated management VLAN only

Compensating: On Linux-based perimeter firewall or the appliance host itself, run: `iptables -I INPUT -p tcp --dport 443 -s -j ACCEPT && iptables -I INPUT -p tcp --dport 443 -j DROP` to whitelist only the management subnet. For Windows-based boundary devices, use `netsh advfirewall firewall add rule name='BLOCK_KACE_EXT' dir=in action=block protocol=tcp localport=443 remoteip=!`. Document the exact timestamp of isolation for later forensic timeline correlation.

Evidence: Before isolating, capture a live netstat snapshot of all active connections to the KACE SMA management interface: `ss -tnp sport = :443` (Linux appliance shell if accessible) or equivalent. Export KACE SMA Apache/nginx access logs from `/var/log/httpd/` or `/var/log/nginx/` — these will show pre-isolation sessions from unauthorized source IPs exploiting the authentication bypass. Capture full packet capture (PCAP) of traffic to/from the KACE SMA management IP using `tcpdump -i eth0 host -w kace_preisolation.pcap` if inline tap is available, to preserve evidence of unauthenticated session tokens.

Step 2: Detection — Review KACE SMA authentication logs for sessions with anomalous user-agent strings, unexpected source IPs, or authentication events lacking corresponding credential validation. Correlate with Active Directory or identity provider logs for accounts showing KACE activity that does not match normal login patterns. Check for new or modified scheduled tasks, scripts, or software distribution packages created through the SMA console by unfamiliar sessions.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Parse KACE SMA web server access logs (typically `/var/log/kace/` or `/data/www/logs/`) using grep to isolate sessions missing standard KACE client user-agent strings: `grep -v 'KACE-Agent\|Mozilla' /var/log/kace/access.log | grep ' 200 '` — successful 200 responses without a legitimate KACE agent or browser UA are high-confidence indicators of bypass exploitation. For AD correlation, run PowerShell on a domain controller: `Get-EventLog -LogName Security -InstanceId 4624,4768,4769 -After (Get-Date).AddDays(-30) | Where-Object {$_.Message -match ''}` to surface Kerberos ticket requests for KACE service accounts from unexpected source IPs. Use osquery with the query `SELECT * FROM scheduled_tasks WHERE path LIKE '%kace%' OR description LIKE '%kace%'` on managed endpoints to detect rogue tasks pushed via the SMA console.

Evidence: Collect KACE SMA authentication audit logs from the admin console (Admin > Logs > Authentication) and export as CSV before any remediation activity — these logs record session tokens, source IPs, and authenticated usernames and will show sessions where authentication succeeded without a corresponding credential challenge, which is the fingerprint of CVE-2025-32975 exploitation. Pull Windows Security Event Log Event ID 4624 (Logon) and 4672 (Special Privileges Assigned) on the KACE SMA host or any Windows-based management server it authenticates against, filtering for the KACE service account during the exposure window. Export the KACE SMA 'Software Distribution' and 'Scripting' module audit trails showing all packages and scripts created or modified, with timestamps and session identifiers, to identify post-exploitation persistence payloads deployed to managed endpoints.

Step 3: Eradication — Apply the patch documented in Quest advisory KB4379499. Confirm the installed KACE SMA version meets or exceeds the remediated version specified in that advisory. Address all four CVEs (CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978) simultaneously, as Quest has bundled the fixes.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If automated patching is unavailable, download the KACE SMA update package directly from the Quest support portal per KB4379499 and apply via the appliance Admin console under Settings > Appliance Updates. Before applying, snapshot the KACE SMA VM (if virtualized) as a forensic baseline using `vmware-cmd snapshot 'pre-patch-forensic'` or equivalent hypervisor CLI. After patching, verify the installed version via the KACE admin console or by running `cat /data/kace/kace_version` (or equivalent appliance shell path) and confirm it matches the remediated version in KB4379499. Run a Nessus or OpenVAS scan (both have free tiers) post-patch targeting the KACE SMA host, checking specifically for CVE-2025-32975 through CVE-2025-32978 to validate fix effectiveness before restoring network access.

Evidence: Before applying the patch, preserve the current KACE SMA appliance configuration export (Admin > Support > Diagnostics Bundle) — this captures the running configuration, installed version string, and active session database, providing a forensic snapshot of the compromised state. Collect the KACE SMA system logs bundle from the admin console, which includes Apache logs, application logs, and authentication records up to the point of patching. Document and hash (SHA-256) any suspicious scripts, packages, or policy objects found in the console during Step 2 review before eradicating them, preserving evidence for potential legal or regulatory proceedings.

Step 4: Recovery — After patching, rotate credentials for all KACE SMA administrator and service accounts. Audit active sessions and revoke any sessions created during the exposure window. Review recently deployed packages, scripts, or policy changes executed through KACE SMA for unauthorized modifications. Confirm KACE SMA authentication logs show only expected login activity post-patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST CM-3 (Configuration Change Control), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Rotate KACE SMA local admin passwords via Admin > Users, enforcing a minimum 16-character random password generated by a password manager (Bitwarden free tier is acceptable). For KACE SMA service accounts in Active Directory, run: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` followed by `Get-ADUser -Properties PasswordLastSet` to confirm rotation. To audit and revoke all active KACE SMA sessions, navigate to Admin > Session Management in the console and terminate all sessions predating the patch timestamp. For endpoint-side verification of unauthorized packages pushed during the exposure window, use osquery: `SELECT name, install_date, install_source FROM programs WHERE install_date > '` across a representative sample of KACE-managed endpoints.

Evidence: Post-rotation, export a fresh KACE SMA authentication log and diff it against the pre-patch export captured in Step 2 to confirm no residual unauthorized sessions persist and that all post-patch logins correspond to known administrators. On KACE-managed Windows endpoints, query for evidence of unauthorized software or scripts deployed during the exposure window using Event ID 11707 (MSI installation) and Event ID 4688 (Process Creation) filtering on processes spawned by the KACE agent service (KSMAAgent.exe or equivalent) — cross-reference timestamps against the confirmed exposure window. Collect a final KACE SMA diagnostics bundle post-recovery as a clean-state forensic baseline for future comparison.

Step 5: Post-Incident — Audit KACE SMA placement in the network architecture. Management appliances with privileged endpoint access should never be internet-facing without strong authentication controls. Evaluate whether multi-factor authentication is enforced for KACE SMA access. Add KACE SMA authentication anomalies to SIEM detection rules. Review the three related CVEs (CVE-2025-32976 through CVE-2025-32978) to identify any additional control gaps exposed by this advisory.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SC-7 (Boundary Protection), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without a commercial SIEM, author a Sigma rule targeting KACE SMA authentication anomalies — specifically, HTTP 200 responses to the KACE authentication endpoint (`/ams/`) from source IPs not in the management VLAN CIDR, or user-agent strings inconsistent with the KACE agent. Use `sigmac` to compile the rule for Elasticsearch or Splunk free tier if available. Subscribe to Quest Security Advisories via the Quest Support portal to receive proactive notification of future KACE SMA CVEs. For MFA enforcement gap, if KACE SMA does not natively support SAML/MFA, place a reverse proxy (Authelia — open source, free) in front of the management interface to enforce TOTP-based MFA before traffic reaches the appliance. Document network segmentation changes made in Step 1 as permanent architecture controls in the organization's network diagram.

Evidence: Conduct a post-incident lessons-learned session within 1–2 weeks per NIST 800-61r3 §4 guidance, documenting the KACE SMA exposure window duration, number of potentially affected managed endpoints, and any confirmed unauthorized actions taken through the console. Produce an artifacts inventory summarizing all forensic evidence collected across Steps 1–4 (PCAPx, log exports, diagnostics bundles, hashed package files) with chain-of-custody documentation in case regulatory reporting or legal action is required. Review CVE-2025-32976 through CVE-2025-32978 technical details (as released by Quest/NVD) to determine whether any additional exploit primitives — such as privilege escalation after authentication bypass via CVE-2025-32975 — were used in combination during the incident.

Detection Guidance

Focus detection on KACE SMA authentication and session logs. Look for: (1) authentication success events with no corresponding password or token validation entry; (2) sessions originating from external or unexpected IP ranges accessing the SMA admin interface; (3) user impersonation patterns where session metadata does not match the impersonated account's known device or location baseline. On the network side, review firewall and proxy logs for direct HTTP/HTTPS connections to KACE SMA management ports from outside trusted management networks. In Active Directory or your identity provider, flag KACE-attributed activity on accounts that have no concurrent authenticated session. Post-exploitation indicators may include new or modified software distribution tasks, changed patch policies, or scheduled scripts added through the SMA console by sessions that cannot be attributed to known administrators. No public IOCs specific to this CVE are confirmed at time of writing; detections should focus on behavioral anomalies rather than known indicators.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2025-32975 - Arctic Wolf	https://arcticwolf.com/resources/blog/cve-2025-32975/	T3
CVE-2025-32975 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-32975	T1

Source	URL	Tier
[PDF] Chubb Vulnerability Alert System – “CVE-2025-32975 Quest KACE ...	https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/busin...	T3
Quest Response to KACE SMA Vulnerabilities: CVE-2025-32975 ...	https://support.quest.com/kb/4379499/quest-response-to-kace-sma-vul...	T3

Generated 2026-04-20 18:51 UTC by TJS Security Command Center