مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of Quest KACE SMA Authentication Bypass Vulnerability

Tracking #:432318651

Date:24-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical authentication bypass vulnerability is being actively exploited in the wild against unpatched Quest KACE Systems Management Appliance (SMA) instances.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability, CVE-2025-32975 (CVSS 10.0), is being actively exploited in the wild against unpatched Quest KACE Systems Management Appliance (SMA) instances.
Threat actors are leveraging this flaw to gain unauthorized administrative access, execute remote commands, deploy malicious payloads, and establish persistence within targeted environments. Organizations with internet-exposed and unpatched SMA systems are at high risk of full system compromise.

Vulnerability Details:

- CVE ID: CVE-2025-32975
- CVSS Score: 10.0 (Critical)
- Vulnerability Type: Authentication Bypass
- Affected Product: Quest KACE Systems Management Appliance

Observed Threat Activity

Security researchers have identified real-world exploitation with the following attack chain:

- Initial Access
  - Exploitation of authentication bypass in exposed SMA instances
  - Unauthorized impersonation of legitimate users
- Execution & Payload Delivery
  - Remote command execution via curl
  - Retrieval of Base64-encoded payloads from attacker-controlled server (216.126.225[.]156)
- Persistence Mechanisms
  - Creation of new administrative accounts
  - Abuse of runkbot.exe (legitimate SMA agent process)
  - Windows Registry modifications via PowerShell scripts
- Post-Exploitation Activities
  - Credential dumping using Mimikatz
  - Network reconnaissance:
    - Enumerating users and admin groups
    - Executing commands like net time, net group
  - Lateral movement:
    - Access to RDP services
    - Targeting backup systems (e.g., Veeam, Veritas) and domain controllers

Patched Versions:

- 13.0.385
- 13.1.81
- 13.2.183
- 14.0.341 (Patch 5)

- 14.1.101 (Patch 4)

RECOMMENDATIONS:

Immediate Actions

- Apply Security Patches Immediately
  - Upgrade to the latest patched SMA versions listed above
- Restrict Internet Exposure
  - Remove SMA instances from public internet access
  - Place behind VPN or zero-trust access controls

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://arcticwolf.com/resources/blog/cve-2025-32975/