

CVE-2025-32975

Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability

CISA KEV since Apr 20, 2026

Actively exploited

Quest KACE Systems Management Appliance (SMA) 13.0.x before 13.0.385, 13.1.x before 13.1.81, 13.2.x before 13.2.183, 14.0.x before 14.0.341 (Patch 5), and 14.1.x before 14.1.101 (Patch 4) contains an authentication bypass vulnerability that allows attackers to impersonate legitimate users without valid credentials. The vulnerability exists in the SSO authentication handling mechanism and can lead to complete administrative takeover.

EVRS 75_{/100} Urgent priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.025 84.5th percentile · FIRST	CISA DEADLINE May 4, 2026 CISA federal deadline · Overdue by 6 months
--	---	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.025 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
kace systems management appliance	≥ 13.0 < 13.0.385 ≥ 13.1 < 13.1.81 ≥ 13.2 < 13.2.183 ≥ 14.0 < 14.0.341 ≥ 14.1 < 14.1.101	13.0.385 · 13.1.81 · 13.2.183 · 14.0.341 · 14.1.101	NVD

Sources

Vendor guidance github.com/advisories/GHSA-hrwx-88rh-95q7

Additional guidance support.quest.com/kb/4379499/quest-response-to-kace-sma-vulnerabilities-cve-2025-32975-cve-2025-32976-cve-2025-32977-cve-2025-32978

NVD nvd.nist.gov/vuln/detail/CVE-2025-32975

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-19028

Current data evulnable.com/vulnerability-management/cve/CVE-2025-32975

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.