CVE-2025-32975 - Quest KACE SMA Authentication Bypass

From: Seralys Research Team via Fulldisclosure <fulldisclosure () seclists org>
Date: Mon, 23 Jun 2025 22:42:51 +0000

```
     Seralys Security Advisory | https://www.seralys.com/research

========================================================================
Title:       Authentication Bypass
Product:     Quest KACE Systems Management Appliance (SMA)
Affected:    Confirmed on 14.1 (older versions likely affected)
Fixed in:    13.0.385, 13.1.81, 13.2.183, 14.0.341(Patch 5),
             14.1.101(Patch 4)
Vendor:      Quest Software
Discovered:  April 2025
Severity:    CRITICAL
CWE:         CWE-287: Improper Authentication
CVE:         CVE-2025-32975
CVSS:        10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Discovered by: Philippe Caturegli & Mohamed Mahmoudi (Seralys)

========================================================================
Overview
--------

Quest KACE SMA 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.

========================================================================
Impact
------

Complete authentication bypass for any valid username
Full administrative access to the appliance
No authentication credentials required

========================================================================
Vendor Response
---------------

Quest has released a fix for this vulnerability as part of a
coordinated disclosure effort. Details and patch availability are
documented in their advisory:
```

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

The issue has been resolved via hotfix or patch in the following KACE SMA versions:

- 13.0.385
- 13.1.81
- 13.2.183
- 14.0.341 (Patch 5)
- 14.1.101 (Patch 4)

Administrators are strongly encouraged to update to one of the patched versions.

==========
Timeline

- 2025-04-14: Initial report submitted to Quest Software
- 2025-04-14: Vendor acknowledged receipt and initiated coordination
- 2025-05-08: Quest shared a preliminary hotfix with Seralys
- 2025-05-17: Seralys confirmed hotfix addressed the reported issues
- 2025-05-27: Quest publicly released the hotfix for CVE-2025-32975
- 2025-06-23: High level public disclosure by Seralys

Note: Detailed technical information and proof-of-concept code will be released after the standard 90-day disclosure period to allow organizations additional time to apply patches.

==========
About Seralys

Seralys is a boutique penetration testing firm with offices in Europe and North America. We provide high value-add penetration testing and security assessments.

https://www.seralys.com

==========
Acknowledgments

Special shoutout to our fellow researchers at BastardLabs. \m/

==========
Disclaimer

This advisory is provided for coordinated disclosure purposes only. Reproduction or distribution for malicious use is strictly prohibited.

EOF

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

CVE-2025-32975 - Quest KACE SMA Authentication Bypass ***Seralys Research Team via Fulldisclosure (Jun 23)***