

Quest



Quest Response to KACE SMA Vulnerabilities: CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978 (4379499)

Title

Quest Response to KACE SMA Vulnerabilities: CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978

Description

During a security review completed by a 3rd party, [Seralys](#), 4 issues were identified. Including one that would allow unauthorized admin access to the appliance.

In partnership with Seralys, Quest has addressed these issues via the supplied hotfix and will be publishing the CVEs in accordance with industry standards, allowing customers time to remediate these issues before they are public.

- CVE-2025-32975
- CVE-2025-32976
- CVE-2025-32977
- CVE-2025-32978

Quest takes handling of vulnerabilities seriously, and we investigate and respond to all reported potential vulnerabilities. Our vulnerability reporting and response process can be found [here](#).

Note: An issue has been identified where in some cases KACE Go app users are unable to login after applying the latest security update patch to the system. **UPDATE:** Cumulative Updates 6 and 5 released for 14.0 and 14.1, respectively. These patches fix the KACE Go app issue mentioned. If on 13.x, please [contact support](#) for assistance.

Cause

CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978 vulnerabilities exist within Quest KACE Systems Management Appliance (SMA) through 14.1 which would allow unauthorized admin access to the appliance.

Resolution

The KACE SMA Vulnerabilities reported under CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978 are resolved in via supplied hotfix or patch on KACE SMA versions **13.0.385, 13.1.81, 13.2.183, 14.0.341 (Patch 5), 14.1.101 (Patch 4)**.

Please make sure the KACE SMA appliance is updated to one of these **secure versions**.

Quest recommends that all customers ensure they are running a supported version of the KACE SMA. See [KACE Software Product Support Lifecycle Policy](#)

How to get the latest KACE SMA security update?

KACE SMA version 13.x:

Please download the [13.x security hotfix](#) available at the support portal and apply under Admin console **Settings | Appliance Updates**.

This update includes SMA 13.0 and 13.1 [2023 security updates](#). Please note the 13.x security hotfix will need to be re-applied to the system every time a full 13.x upgrade is completed to remain secure.
i.e. 13.1.79 -> 13.1.81 (security update) -> 13.2.182 -> 13.2.183 (security update).

KACE SMA version 14.0 and later:

Please get the latest version available for [download at the support portal](#) or using the automatic update through your KACE SMA adminui **Settings | Appliance Updates - Server Version & Updates**.

If manually upgrading from 14.0.341 please make sure the latest version (14.1.101) is downloaded and applied.
Upgrades from 14.0.341 to 14.1.95 are not supported.

If the update does not show available for your appliance, please see: [KACE Auto Update does not find the automatic update but the release can be found on the download page](#)

★ Recommended Content**Product(s):**

KACE Asset Management Appliance

14.1, 14.0, 13.1.80, 13.2, 13.1.79

KACE Service Desk

14.1, 14.0, 13.1.80, 13.2, 13.1.79

KACE Systems Management Appliance

14.1, 14.0, 13.1.80, 13.2, 13.1.79

KACE as a Service

14.1, 14.0, 13.1.80, 13.2, 13.1.79

Topic(s):

Configuration

Article History:

Created on: 5/27/2025

Last Update on: 6/19/2025

Search All Articles

