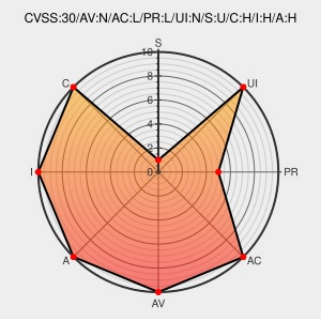
CVE-2018-11134

Published on: 05/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11134

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Kace System Management Appliance from Quest contain the following vulnerability:

In order to perform actions that requires higher privileges, the Quest KACE System Management Appliance 8.0.318 relies on a message queue managed that runs with root privileges and only allows a set of commands. One of the available commands allows changing any user's password (including root). A low-privilege user could abuse this feature by changing the password of the 'kace_support' account, which comes disabled by default but has full sudo privileges.

CVE-2018-11134 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Quest KACE System Management Appliance	Exploit	MISC www.coresecurity.com/advisories/quest-kace

Quest KACE System Management Appliance Multiple Vulnerabilities | SecureAuth	Exploit Technical Description Third Party Advisory www.coresecurity.com text/html	MISC www.coresecurity.com/advisories/quest-kace-system-management-appliance-multiple-vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quest	Kace System Management Appliance	8.0.318	All	All	All
Application	Quest	Kace System Management Appliance	8.0.318	All	All	All

cpe:2.3:a:quest:kace_system_management_appliance:8.0.318:*:*:*:*:*:*:*:

cpe:2.3:a:quest:kace_system_management_appliance:8.0.318:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→