Bug 1962908 (CVE-2021-3563) - CVE-2021-3563 Keystone: Verification of application credentials is silently length-limited

Keywords: Security ×

Status: NEW

Alias: CVE-2021-3563

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 1964525 2070962 2154112 1964527 1964529

Blocks: 1922882 1963091

TreeView+ depends on / blocked

Reported: 2021-05-20 18:41 UTC by Nick Tait

Modified: 2022-12-15 21:38 UTC (History)

CC List: 16 users (show)

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: A flaw was found in openstack-keystone. Only the first 72 characters of an application secret are verified allowing attackers bypass some password complexity which administrators may be counting on. The highest threat from this vulnerability is to data confidentiality and integrity.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Nick Tait 2021-05-20 18:41:05 UTC Description

Keystone only verifies part of the secret - the first 72 characters. Additional complexity is ignored, giving users an inflated sense of security. Default length of a secret seems to be 86 characters. While brute forcing at this scale is out of reach for many attackers, state of the art is constantly evolving and we need to support OpenStack for many years to come.

Jan Zerebecki 2021-06-09 13:43:11 UTC Comment 4

Upstream report is https://bugs.launchpad.net/keystone/+bug/1901891

Note

You need to log in before you can comment on or make changes to this bug.