Issues regarding application credentials

Bug #1901891 reported by Arjen on 2020-10-28

This bug affects 1 person 10

Affects	Status	Importance	Assigned to	Milestone
OpenStack Identity (keystone)	In Progress	Undecided	David Wilde	
OpenStack Security Advisory	Won't Fix	Undecided	Unassigned	

Bug Description

```
While looking into the application credential API we came across several
issues. Since they are all closely related I will file them under this
issue:

- No secret strength requirements. To configure a password strength
requirement for users, one can use `password_regex`. However, this is not
possible for application credentials, which makes it possible to create a
credentials with the secret 'a':

$ openstack application credential create test-secret-strength --secret a
+--------------+----------------------------------+
| Field | Value |
+--------------+----------------------------------+
| description | None |
| expires_at | None |
| id | xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx |
| name | test-secret-strength |
| project_id | xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx |
| roles | member reader |
| secret | a |
| system | None |
| unrestricted | False |
| user_id | xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx |
+--------------+----------------------------------+

To attack this, you'd still need to know the ID, but combined with https:/
/bugs.launchpad.net/keystone/+bug/1901207 the impact of this issue is
increased.

- No lockout feature. For normal login, the settings `lockout_failure_
attempts` and `lockout_duration` are used. These do not affect the
application credential API. This increases the attack surface
unnecessarily in my opinion. Combined with weak secrets and https:/
/bugs.launchpad.net/keystone/+bug/1901207 the probability of a successful
attack is increased.

- Only part of secret is verified. It looks like only the first 72
characters of the secret of an application credential are used to verify
it. Characters after that are not used in the verification. The default
length of a secret seems to be 86 characters. Even though brute forcing 72
characters is still pretty impossible, this doesn't sound like intended
behaviour to me.
```

See original description

Tags: security

CVE References

2021-3563

Jeremy Stanley (Fungi) wrote on 2020-10-28: #1

```
Since this report concerns a possible security risk, an incomplete
security advisory task has been added while the core security
reviewers for the affected project or projects confirm the bug and
discuss the scope of any vulnerability along with potential
solutions.

description:updated
Changed in ossa:
     status:New → Incomplete
```

Jeremy Stanley (Fungi) wrote on 2020-10-28: #2

```
Breaking down the list of issues here with proposed report
classifications:

1. (D/security hardening) request to implement secret strength
requirements for app credentials

2. (D/security hardening) request to implement brute-force mitigation via
lockout for app credentials

3. (C1/impractical) app credentials are truncated to 72 characters prior
to comparison

[ report taxonomy: https://security.openstack.org/vmt-process.
html#incident-report-taxonomy ]

For #1 and #2 I'm assuming the Keystone docs don't claim application
credentials provide these protections currently, and so they're
effectively security-related feature requests. #3 could be construed as a
defect worthy a CVE assignment, but as vulnerabilities go it's fairly
impractical to exploit as you note, so I don't think we need to issue any
advisory for it. Also it doesn't seem to me that any of these items need
to be discussed in private under embargo, so we could switch this bug to
public. Does anyone strongly disagree with the above assessment?
```

Gage Hugo (gagehugo) wrote on 2021-01-21: #3

Agreed with bug report and Jeremy, there doesn't seem to be anything directly exploitable here, we can make this public.

1 & 2 seem to be requests for security hardening similar to how keystone handles PCI-DSS features for user passwords. 3 might indeed be unintended behavior and should be investigated.

description:updated
information type:Private Security → Public Security

Jeremy Stanley (fungi) wrote on 2021-02-17: #4

Given nobody has objected to the proposed classifications in my comment #2 from October, I'll go ahead and mark our security advisory task Won't Fix for this. We can revisit the decision if anyone disagrees.

Changed in ossa:
status:Incomplete → Won't Fix
information type:Public Security → Public
tags:added: security

Nick Tait (nickthetait) wrote on 2021-03-03: #5

I'm with Gage on classifications. Should #3 be split into its own bug report for keystone?

Nick Tait (nickthetait) wrote on 2021-04-23: #6

Checking back in, #3 deserves a CVE IMO. Happy to assign that on Red Hat's behalf. WDYT Gague?

Gage Hugo (gagehugo) wrote on 2021-04-23: #7

Anyone can request a CVE, feel free to request one for this.

As Jeremy pointed out, #3 is pretty impossible to exploit, so we likely won't issue an advisory.

Arjen (arjentz) wrote on 2021-04-28: #8

Even though successfully exploiting #3 is pretty unlikely, I personally do agree a CVE would be applicable. I feel it'd be appropriate if Red Hat would request it rather than myself.

Nick Tait (nickthetait) wrote on 2021-05-21: #9

CVE-2021-3563 has been assigned to #3.

Arjen, is it OK to list you as the reporter? What name should I use? Are you affiliated with an organization?

Nick Tait (nickthetait) wrote on 2021-05-21: #10

https://access.redhat.com/security/cve/CVE-2021-3563

Arjen (arjentz) wrote on 2021-05-21: #11

Yes, that is OK. You can use my name as: Arjen T. Zijlstra.

At the time I was working at Warpnet, which I would be fine with to be added, but I recently started a new job so for me it's not a necessity to list as employer.

Nick Tait (nickthetait) wrote on 2021-05-25: #12

Appreciate the report, I've added you.

OpenStack Infra (hudson-openstack) wrote on 2021-08-05: **Fix proposed to keystone (master)** #13

Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/keystone/+/803641

Changed in keystone:
status:New → In Progress

Lance Bragstad (lbragstad) wrote on 2021-08-05: #14

I was able to verify the hash truncation issue using a functional test in keystone [0].

We can re-use that test moving forward to develop a fix.

[0] https://review.opendev.org/c/openstack/keystone/+/803641

David Wilde (dave-wilde) on 2022-02-10

Changed in keystone:
assignee:nobody → David Wilde (dave-wilde)

Luis Flores (luis-flores-ibm) wrote on 2022-10-31: #15

There is an update about the fix for this vulnerability ?

See full activity log

To post a comment you must log in.

Jordan Rinke
Joshua Padman
Jun Hong Li
Kausal Malladi
Kausum Kumar
Ken'ichi Ohmichi
Kenji Motohashi
Kent Liu
Kristi Nikolla
Kunal.Yadav
LIU Yulong
Lance Bragstad
Le Tian Ren
Lei Zhang
Louis Fourie
Lshutao
Lukas Koenen
Madhu CR
Malini Bhandaru
Mamta Jha
Manikantha Sriniv...
Manoj Raju
Marcus Vinicius G...
Margaret Eker
Mark McLoughlin
Matthew Thode
Matthieu Huin
Meera Belur
Michael Rowland H...
Mika Kohonen
Mikhail Nikolaenko
Mohankumar
Mohit
Nachiappan
Naved Ali
Naved Ali Shah
Normen Scholtke
Pablo Cortijo
Pankaj Mishra
Paul Voccio
Pavani_addanki
Perry Waldner
Pradeep Roy Kandru
Prateek
Priti Desai
Prosunjit Biswas
Rafi Khardalian
Raildo Mascena de...
Rajesh Battala
Raju Alluri
Ranjit Ray
Richa
Rick Melick
Rochelle Grober
Ron Cannella
Ryo Shi
Satyanarayana Pat...
Sayaji Patil
Sebastian Luna-Va...
Shawn Hartsock
Shen Yang
Shruthi Chari
Shuo Liu
Sid Sun
Songhee Kang
Soo Choi
Steve Sloka
Steven Pavlon
Steven Relf
Stuart Hart
Summer Long
Swaroop Jayanthi
Tao Zhou
Taurus Cheung
Tayaa Med Amine
Thongth
Tiago Everton Fer...
Tiago Martins
Tony Wolf
Tushar Patil
Uma
Vidhisha Nair
Vikram
Vil Surkin
Vinu Pillai
Vishakha Agarwal
Xiang Hui
Xiaojun Lin
Xin Zhong
Xingchao Yu

Yahoo! Engineerin...
Yongqiang Yang
Zahid Hasan
ZhangNi
Ziv
ammarun
anndy
armyman420
avinashsau
brightson
bugtracker@devshe...
chaiwat wannaposop
chitu
congge
devin.li
dominic_chen
ekotkaj
fei Yang
galeido
gsccc
iopenstack
jeff wang
joel BELAFA
kalim khuang
kgrvamsi
lanpi
laoyi
lei zhang
liaonanhai
lololmarwa255
lpmqtt
maestropandy
manish
mershard frierson
miralaunchpad
mohit.048
nawawit kes
raja
satyanarayana pat...
satyanarayana pat...
sivagnanam C
sunilcn
tangfeixiong
truijllo
vivek.ys
wanghuagong
xiaoningli
xreuze
yangbo
yangzhenyu
zhangqinta
zzfancy