

Pulp - Backport #8540

pulpcore 3.7 branch needs PyYAML dep raised to include 5.4.x to fix CVE-2020-14343 (backport 205c903bb22)

04/09/2021 10:27 PM - alikins

Status: MODIFIED	Start date:
Priority: Normal	Due date:
Assignee: ttereshc	% Done: 100%
Category:	Estimated time: 0:00 hour
Sprint/Milestone: 3.7.5	Sprint: Sprint 94
Triaged: No	Quarter: Q2-2021
Sprint Candidate: No	
Tags:	
Description	
Backport request for 205c903bb2232d7f6fb8291c2f6ab0ba74442f9e into 3.7 branch, maybe others.	
CVE-2020-14343 (Improper Input Validation in PyYAML)	
<ul style="list-style-type: none">https://github.com/advisories/GHSA-8q59-q68h-6hv4https://nvd.nist.gov/vuln/detail/CVE-2020-14343https://github.com/yaml/pyyaml/issues/420#issuecomment-663673966	
pulpcore 3.7 branch (and latest release 3.7.4) have PyYaml dep:	
PyYAML>=5.1.1,<5.4.0	
which prevents updating to PyYaml 5.4.1	
Related issues:	
Related to Pulp - Issue #8539: pulpcore 3.7 branch needs PyYAML dep raised to...	CLOSED - DUPLICATE

Associated revisions

Revision d0e87121 - 04/12/2021 12:15 PM - ttereshc

Allow to use PyYAML 5.4 which addresses CVE-2020-14343

<https://github.com/advisories/GHSA-8q59-q68h-6hv4><https://nvd.nist.gov/vuln/detail/CVE-2020-14343>

closes #8540 <https://pulp.plan.io/issues/8540>

History

#1 - 04/09/2021 10:31 PM - ggaaney

- Related to Issue #8539: pulpcore 3.7 branch needs PyYAML dep raised to include 5.4.x to fix CVE-2020-14343 added

#2 - 04/12/2021 10:28 AM - ttereshc

- Status changed from NEW to ASSIGNED

- Assignee set to ttereshc

- Sprint set to Sprint 94

- Quarter set to Q2-2021

#3 - 04/12/2021 11:44 AM - pulpbot

- Status changed from ASSIGNED to POST

PR: <https://github.com/pulp/pulpcore/pull/1253>

#4 - 04/12/2021 11:58 AM - ttereshc

- Sprint/Milestone set to 3.7.5

#5 - 04/12/2021 12:15 PM - ttereshc

- Status changed from *POST* to *MODIFIED*

- % Done changed from 0 to 100

Applied in changeset [pulpcore|d0e87121a49a6102a1c6985a48bc308a6cda4c72](#).