Pulp - Issue #1834

CVE-2016-3112: Pulp consumer private keys are world-readable

04/11/2016 02:50 PM - jcline@redhat.com

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	jcline@redhat.com	**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	1. Low	**Groomed:**	No
Version:		**Sprint Candidate:**	No
Platform Release:	2.8.3	**Tags:**	Pulp 2
OS:		**Sprint:**	
Triaged:	Yes	**Quarter:**	

Description

Pulp consumers write the certificate and private key issued by the Pulp server's registration process to /etc/pki/pulp/consumer/consumer-cert.pem with 644 permissions, which allowed anyone on the host to read the private key.

This means a non-privileged user on the host could authenticate with the Pulp server as the consumer.

Associated revisions

Revision 707a39cb - 04/13/2016 08:01 PM - Jeremy Cline

Create consumer private keys with 600 permissions (CVE-2016-3112)

Prior to this commit, consumers wrote the certificate and private key issued by the Pulp server's registration process to /etc/pki/pulp/consumer/consumer-cert.pem with 644 permissions, which allowed anyone on the host to read the private key. This ensures the file is written with 600 permissions.

https://pulp.plan.io/issues/1834

fixes #1834

Revision 707a39cb - 04/13/2016 08:01 PM - Jeremy Cline

Create consumer private keys with 600 permissions (CVE-2016-3112)

Prior to this commit, consumers wrote the certificate and private key issued by the Pulp server's registration process to /etc/pki/pulp/consumer/consumer-cert.pem with 644 permissions, which allowed anyone on the host to read the private key. This ensures the file is written with 600 permissions.

https://pulp.plan.io/issues/1834

fixes #1834

Revision e152f9e1 - 04/19/2016 08:46 PM - rbarlow

Add release notes for the upcoming 2.8.3.

re #1827 re #1830 re #1833 re #1834 re #1837

Credit goes to Jeremy Cline for writing the included release notes for CVE-2016-3111 and CVE-2016-3112.

Revision e152f9e1 - 04/19/2016 08:46 PM - rbarlow

Add release notes for the upcoming 2.8.3.

re #1827 re #1830 re #1833 re #1834 re #1837

Credit goes to Jeremy Cline for writing the included release notes for CVE-2016-3111 and CVE-2016-3112.

History

#1 - 04/11/2016 02:50 PM - jcline@redhat.com

- Private changed from No to Yes

#2 - 04/13/2016 06:50 PM - jcline@redhat.com

- Subject changed from reserved to Pulp consumer private keys are world-readable

- Description updated

- Private changed from Yes to No

https://github.com/pulp/pulp/pull/2531

#3 - 04/13/2016 07:00 PM - jcline@redhat.com

- Status changed from NEW to POST

- Assignee set to jcline@redhat.com

#4 - 04/13/2016 07:58 PM - semyers

- Platform Release set to 2.8.3

#5 - 04/13/2016 08:00 PM - semyers

- Subject changed from Pulp consumer private keys are world-readable to CVE-2016-3112: Pulp consumer private keys are world-readable

#6 - 04/13/2016 08:25 PM - Anonymous

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulp|707a39cb3504a55ce36cae15b19ad1b3f4146a36.

#7 - 04/15/2016 05:11 PM - mhrivnak

- Priority changed from Normal to High

- Severity changed from 2. Medium to 1. Low

- Triaged changed from No to Yes

#8 - 04/27/2016 12:39 AM - semyers

- Status changed from MODIFIED to 5

#9 - 05/17/2016 09:31 PM - semyers

- Status changed from 5 to CLOSED - CURRENTRELEASE

#10 - 04/15/2019 10:32 PM - bmbouter

- Tags Pulp 2 added