Pulp - Issue #1837

CVE-2016-3111: pulp.spec generates its RSA keys for message signing insecurely

04/12/2016 04:15 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

During installation, the RSA key pairs used to validate messages between the pulp server and pulp consumers are generated in a directory that is world-readable with a umask of 002. After it was written, the permissions are modified to protect the key. For a brief moment, the RSA keys are world-readable. An attacker who has access to the host installing Pulp could theoretically open the file after it is created, but before its permissions are set, and read the private key.

Associated revisions

Revision 20955f6f - 04/13/2016 08:06 PM - Jeremy Cline

pulp.spec now generate RSA keys with umask 077 (CVE-2016-3111)

During installation, the RSA key pairs used to validate messages between the pulp server and pulp consumers were generated in a directory that is world-readable with a umask of 002. After it was written, the permissions were modified to protect the key. For a brief moment, the RSA keys were world-readable. This commit explicitly sets the umask in the %post scriptlet to be 077 so it is only readable to the owner.

https://pulp.plan.io/issues/1837

fixes #1837

Revision 20955f6f - 04/13/2016 08:06 PM - Jeremy Cline

pulp.spec now generate RSA keys with umask 077 (CVE-2016-3111)

During installation, the RSA key pairs used to validate messages between the pulp server and pulp consumers were generated in a directory that is world-readable with a umask of 002. After it was written, the permissions were modified to protect the key. For a brief moment, the RSA keys were world-readable. This commit explicitly sets the umask in the %post scriptlet to be 077 so it is only readable to the owner.

https://pulp.plan.io/issues/1837

fixes #1837

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 - 04/13/2016 06:44 PM - jcline@redhat.com

- Subject changed from reserved to pulp.spec generates its RSA keys for message signing insecurely

- Description updated

https://github.com/pulp/pulp/pull/2530

#2 - 04/13/2016 06:44 PM - jcline@redhat.com

- Private changed from Yes to No

#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.spec generates its RSA keys for message signing insecurely to CVE-2016-3111: pulp.spec generates its RSA keys for message signing insecurely

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

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulp|20955f6fa1e7a3ab3c155cb3ce00bff5b615bd3a.

#7 - 04/15/2016 05:16 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