Pulp - Issue #1827

CVE-2016-3106: Insecure creation of temporary directory when generating new CA key

04/08/2016 05:10 PM - rbarlow

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	rbarlow	**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	2. Medium	**Groomed:**	No
Version:		**Sprint Candidate:**	No
Platform Release:	2.8.3	**Tags:**	Pulp 2
OS:		**Sprint:**	
Triaged:	Yes	**Quarter:**	

Description

The pulp-gen-ca-certificate script created
the Pulp CA certificate and key in /tmp/$RANDOM. This led to about
32,768 possible directories. Florian Weimer and Sander Bos
notified the Pulp team that if a user happened to own a directory
that the script chose, the user would be able to read the
certificate authority certificate. Additionally, both security
researchers concluded that there is a race condition between
creating the secure folder and the later chmod, during which an
attacker could read and hold open the inode for the $TMP
directory. This would allow an attacker to read the key that is
later written.

Sander Bos additionally concluded that an attacker could create a
DoS attack two ways: 0) By creating a symlink within the $TMP
directory that points at an important system resource, such as
/etc/passwd, or 1) By creating $TMP itself as a symlink to /,
which would cause / to be chmod'd to 0700 later in the script.

The fix adjusts the script to use mktemp -d to ensure that a
unique and safe directory is used to create the Pulp CA
certificate. Additionally, the script uses set -e so that it will
halt if there are errors.

Thanks to Florian Weimer and to Sander Bos for independently
notifying Pulp of the issue and for suggesting the needed changes
to fix it. Thanks to Adam Mariš for advising the Pulp team through
the fix. The Pulp team is thankful to the security community for
their thoughtful analysis, and for taking the time to report these
issues.

Associated revisions

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.

Revision 0b23e8f1 - 04/21/2016 04:48 PM - rbarlow

Safely create the dir in which the CA is created (CVE-2016-3106).

Prior to this commit, the pulp-gen-ca-certificate script created the Pulp CA certificate and key in /tmp/$RANDOM. This led to about 32,768 possible directories. Florian Weimer and Sander Bos notified the Pulp team that if a user happened to own a directory that the script chose, the user would be able to read the certificate authority certificate. Additionally, both security researchers concluded that there is a race condition between creating the secure folder and the later chmod, during which an attacker could read and hold open the inode for the $TMP directory. This would allow an attacker to read the key that is later written.

Sander Bos additionally concluded that an attacker could create a DoS attack two ways: 0) By creating a symlink within the $TMP directory that points at an important system resource, such as /etc/passwd, or 1) By creating $TMP itself as a symlink to /, which would cause / to be chmod'd to 0700 later in the script.

This commit adjusts the script to use mktemp -d to ensure that a unique and safe directory is used to create the Pulp CA certificate. Additionally, the script uses set -e so that it will halt if there are errors.

Thanks to Florian Weimer and to Sander Bos for independently notifying Pulp of the issue and for suggesting the needed changes to fix it. Thanks to Adam Mariš for advising the Pulp team through the fix. The Pulp team is thankful to the security community for their thoughtful analysis, and for taking the time to report these issues.

https://pulp.plan.io/issues/1827

fixes #1827

Revision 0b23e8f1 - 04/21/2016 04:48 PM - rbarlow

Safely create the dir in which the CA is created (CVE-2016-3106).

Prior to this commit, the pulp-gen-ca-certificate script created the Pulp CA certificate and key in /tmp/$RANDOM. This led to about 32,768 possible directories. Florian Weimer and Sander Bos notified the Pulp team that if a user happened to own a directory that the script chose, the user would be able to read the certificate authority certificate. Additionally, both security researchers concluded that there is a race condition between creating the secure folder and the later chmod, during which an attacker could read and hold open the inode for the $TMP directory. This would allow an attacker to read the key that is later written.

Sander Bos additionally concluded that an attacker could create a DoS attack two ways: 0) By creating a symlink within the $TMP directory that points at an important system resource, such as /etc/passwd, or 1) By creating $TMP itself as a symlink to /, which would cause / to be chmod'd to 0700 later in the script.

This commit adjusts the script to use mktemp -d to ensure that a unique and safe directory is used to create the Pulp CA certificate. Additionally, the script uses set -e so that it will halt if there are errors.

Thanks to Florian Weimer and to Sander Bos for independently notifying Pulp of the issue and for suggesting the needed changes to fix it. Thanks to Adam Mariš for advising the Pulp team through the fix. The Pulp team is thankful to the security community for their thoughtful analysis, and for taking the time to report these issues.

https://pulp.plan.io/issues/1827

fixes #1827

History

#1 - 04/13/2016 06:41 PM - rbarlow

- Subject changed from reserved to CVE-2016-3106: Insecure creation of temporary directory when generating new CA key

- Status changed from NEW to ASSIGNED

- Assignee set to rbarlow

- Private changed from Yes to No

- Triaged changed from No to Yes

#2 - 04/13/2016 06:42 PM - rbarlow

- Description updated

#3 - 04/13/2016 06:42 PM - rbarlow

- Status changed from ASSIGNED to POST

- Platform Release set to 2.8.3

https://github.com/pulp/pulp/pull/2527

#4 - 04/13/2016 07:07 PM - rbarlow

https://github.com/pulp/pulp/pull/2532

#5 - 04/21/2016 04:54 PM - rbarlow

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulp|0b23e8f1627e56a0157a68fbafc40e92be2936d0.

#6 - 04/27/2016 12:38 AM - semyers

- Status changed from MODIFIED to 5

#7 - 05/17/2016 09:31 PM - semyers

- Status changed from 5 to CLOSED - CURRENTRELEASE

#8 - 04/15/2019 10:32 PM - bmbouter

- Tags Pulp 2 added