Pulp - Issue #1830

CVE-2016-3108: Insecure temporary file used when generating certificate for Pulp Nodes

04/08/2016 09:23 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

Security researcher Sander Bos contacted the Pulp team to notify us that the pulp-gen-nodes-certificate script suffers from the same exploit as was found in CVE-2016-3095, namely that the $TMP directory that contains the Nodes private key was created in an unsafe manner. The fix is to use mktemp -d to safely create the directory.

Thanks to Sander Bos for taking the time to carefully inspect the Pulp codebase and for writing a wonderfully detailed report describing the issue and the fix for it.

Credit also goes to Jeremy Cline (Red Hat) for independently reporting this issue.

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 8571d9a0 - 04/21/2016 04:55 PM - rbarlow

CVE-2016-3107 & CVE-2016-3108: Safely generate Nodes certificate.

This commit fixes two CVEs.

CVE-2016-3107

Install Node certificate with 640, apache owned (CVE-2016-3107).

Prior to this commit, the Node certificate had been installed world-readable:

$ ls -lah /etc/pki/pulp/nodes/ total 4.0K drwxr-xr-x. 2 root root 21 Apr 8 16:37 . drwxr-xr-x. 4 root root 90 Apr 8 16:37 .. -rw-r--r--. 1 root root 3.2K Apr 8 16:37 node.crt

This commit adjusts the generation script to limit the permissions to 0640, and to adjust the group ownership to the apache group.

Credit also goes to Jeremy Cline (Red Hat) for independently discovering and reporting this issue.

https://pulp.plan.io/issues/1833

fixes #1833

CVE-2016-3108

Safely create tmp dir for the Nodes certificate (CVE-2016-3108).

Security researcher Sander Bos contacted the Pulp team to notify us that the pulp-gen-nodes-certificate script suffers from the same exploit as was found in CVE-2016-3095, namely that the $TMP directory that contains the Nodes private key was created in an unsafe manner. This commit contains his proposed fix to use mktemp -d to safely create the directory.

Additionally, I added a set -e so that the script would exit upon error.

Thanks to Sander Bos for taking the time to carefully inspect the Pulp codebase and for writing a wonderfully detailed report describing the issue and the fix for it.

Credit also goes to Jeremy Cline (Red Hat) for independently reporting this issue.

https://pulp.plan.io/issues/1830

fixes #1830

Revision 8571d9a0 - 04/21/2016 04:55 PM - rbarlow

CVE-2016-3107 & CVE-2016-3108: Safely generate Nodes certificate.

This commit fixes two CVEs.

CVE-2016-3107

Install Node certificate with 640, apache owned (CVE-2016-3107).

Prior to this commit, the Node certificate had been installed world-readable:

$ ls -lah /etc/pki/pulp/nodes/ total 4.0K drwxr-xr-x. 2 root root 21 Apr 8 16:37 . drwxr-xr-x. 4 root root 90 Apr 8 16:37 .. -rw-r--r--. 1 root root 3.2K Apr 8 16:37 node.crt

This commit adjusts the generation script to limit the permissions to 0640, and to adjust the group ownership to the apache group.

Credit also goes to Jeremy Cline (Red Hat) for independently discovering and reporting this issue.

https://pulp.plan.io/issues/1833

fixes #1833

CVE-2016-3108

Safely create tmp dir for the Nodes certificate (CVE-2016-3108).

Security researcher Sander Bos contacted the Pulp team to notify us that the pulp-gen-nodes-certificate script suffers from the same exploit as was found in CVE-2016-3095, namely that the $TMP directory that contains the Nodes private key was created in an unsafe manner. This commit contains his proposed fix to use mktemp -d to safely create the directory.

Additionally, I added a set -e so that the script would exit upon error.

Thanks to Sander Bos for taking the time to carefully inspect the Pulp codebase and for writing a wonderfully detailed report describing the issue and the fix for it.

Credit also goes to Jeremy Cline (Red Hat) for independently reporting this issue.

https://pulp.plan.io/issues/1830

fixes #1830

History

#1 - 04/13/2016 06:55 PM - rbarlow

- Subject changed from reserved to CVE-2016-3108: Insecure temporary file used when generating certificate for Pulp Nodes

- Description updated

- Status changed from NEW to POST

- Assignee set to rbarlow

- Private changed from Yes to No

- Triaged changed from No to Yes

https://github.com/pulp/pulp/pull/2528

#2 - 04/13/2016 07:08 PM - rbarlow

https://github.com/pulp/pulp/pull/2533

#3 - 04/13/2016 07:58 PM - semyers

- Platform Release set to 2.8.3

#4 - 04/18/2016 11:28 PM - rbarlow

https://github.com/pulp/pulp/pull/2543

#5 - 04/18/2016 11:31 PM - rbarlow

https://github.com/pulp/pulp/pull/2544

#6 - 04/21/2016 04:56 PM - rbarlow

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulp|8571d9a0cd7a7cb68c8e8640d01bfbd3560509cf.

#7 - 04/27/2016 12:38 AM - semyers

- Status changed from MODIFIED to 5

#8 - 05/17/2016 09:31 PM - semyers

- Status changed from 5 to CLOSED - CURRENTRELEASE

#9 - 04/15/2019 10:32 PM - bmbouter

- Tags Pulp 2 added