Pulp - Issue #1858

CVE-2016-3704: Unsafe use of bash $RANDOM for NSS DB password and seed

04/22/2016 11:11 PM - rbarlow

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	rbarlow	**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	3. High	**Groomed:**	No
Version:		**Sprint Candidate:**	No
Platform Release:	2.8.5	**Tags:**	Pulp 2
OS:		**Sprint:**	
Triaged:	Yes	**Quarter:**	

Description

In working on another security issue in this same script, I noticed that Pulp's pulp-qpid-ssl-cfg script uses bash's $RANDOM in unsafe ways. One of them is already being fixed as part of another CVE (the TMP directory is unsafe, CVE-2016-3696), but the other two uses are:

0) The default NSS DB password is a single value from $RANDOM, limiting it to the strings from 0 to 32768:

https://github.com/pulp/pulp/blob/pulp-2.8.2-1/server/bin/pulp-qpid-ssl-cfg#L25

1) The certutil -z flag receives a "noise file". The script uses $RANDOM to populate a file with numbers to generate this file:

https://github.com/pulp/pulp/blob/pulp-2.8.2-1/server/bin/pulp-qpid-ssl-cfg#L97-L105

Since $RANDOM is used in this way, the seed file ends up having low diversity since only 11 possible bytes appear in the file: ASCII 0-9 and newline. Additionally, bash's RANDOM has not been described as a sound random generator for such purposes.

pwgen can be used to fix #0, but I'm not sure we want to depend on pwgen. One possibility is to avoid having a default password and force the user to provide one. Suggestions for this problem welcome.

For #1 we should just grab 8 kB from /dev/urandom and call it a day.

Associated revisions

Revision 1b9b635d - 05/03/2016 08:35 PM - rbarlow

CVE-2016-3704: Use stronger seed and DB password. (#2555)

Pulp's pulp-qpid-ssl-cfg script used bash's $RANDOM in unsafe ways:

1. The default NSS DB password was a single value from $RANDOM, limiting it to the strings from 0 to 32768.
2. The certutil -z flag receives a "noise file". The script used $RANDOM to populate a file with numbers to generate this file. Since $RANDOM was used in this way, the seed file had low diversity since only 11 possible bytes appeared in the file (ASCII 0-9 and newline).

This commit alters the script to use /dev/urandom as the source for generating the DB password and the seed.

https://pulp.plan.io/issues/1858

fixes #1858

Revision 1b9b635d - 05/03/2016 08:35 PM - rbarlow

CVE-2016-3704: Use stronger seed and DB password. (#2555)

Pulp's pulp-qpid-ssl-cfg script used bash's $RANDOM in unsafe ways:

1. The default NSS DB password was a single value from $RANDOM, limiting it to the strings from 0 to 32768.
2. The certutil -z flag receives a "noise file". The script used $RANDOM to populate a file with numbers to generate this file. Since $RANDOM was used in this way, the seed file had low diversity since only 11 possible bytes appeared in the file (ASCII 0-9 and newline).

This commit alters the script to use /dev/urandom as the source for generating the DB password and the seed.

https://pulp.plan.io/issues/1858

fixes #1858

Revision d86b111b - 05/23/2016 07:00 PM - Randy Barlow

Add release notes for the CVEs included with Pulp 2.8.4.

re #1854 re #1858

Revision d86b111b - 05/23/2016 07:00 PM - Randy Barlow

Add release notes for the CVEs included with Pulp 2.8.4.

re #1854 re #1858

History

#1 - 04/22/2016 11:14 PM - rbarlow

- Description updated

#2 - 04/22/2016 11:15 PM - rbarlow

- Description updated

#3 - 04/22/2016 11:18 PM - rbarlow

- Severity changed from 2. Medium to 3. High

#4 - 04/23/2016 12:52 AM - rbarlow

- Description updated

#5 - 04/24/2016 08:52 PM - rbarlow

- Subject changed from CVE-2016-XXXX: Unsafe use of bash $RANDOM for NSS DB password and seed to CVE-2016-3700: Unsafe use of bash $RANDOM for NSS DB password and seed

#6 - 04/25/2016 09:02 PM - rbarlow

- Subject changed from CVE-2016-3700: Unsafe use of bash $RANDOM for NSS DB password and seed to CVE-2016-3704: Unsafe use of bash $RANDOM for NSS DB password and seed

#7 - 04/25/2016 11:20 PM - rbarlow

- Status changed from ASSIGNED to POST

https://github.com/pulp/pulp/pull/2555

#8 - 04/26/2016 04:21 AM - rbarlow

- Platform Release set to 2.8.4

#9 - 04/29/2016 04:50 PM - dkliban@redhat.com

- Triaged changed from No to Yes

#10 - 05/03/2016 08:35 PM - rbarlow

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulp|1b9b635d370b3103376f6fb7864e76181a6f0f20.

#11 - 05/26/2016 10:06 PM - semyers

- Status changed from MODIFIED to 5

#12 - 05/31/2016 06:58 PM - semyers

- Platform Release changed from 2.8.4 to 2.8.5

#13 - 05/31/2016 07:00 PM - semyers

- Status changed from 5 to MODIFIED

#15 - 06/17/2016 07:05 PM - semyers

- Status changed from MODIFIED to 5

#16 - 06/27/2016 06:58 PM - semyers

- Status changed from 5 to CLOSED - CURRENTRELEASE

#18 - 04/15/2019 10:31 PM - bmbouter

- Tags Pulp 2 added