Foreman - Feature #29960

Run foreman.service with systemd PrivateTmp=true

05/29/2020 01:26 PM - Anurag Patel

Status:	Closed		
Priority:	High		
Assignee:	Evgeni Golov		
Category:	Packaging		
Target version:	2.4.0		
Difficulty:		**Fixed in Releases:**	2.4.0
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:	1732038	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/8345, https://github.com/theforeman/foreman/pull/8351, https://github.com/theforeman/foreman/pull/8356		

Description

When foreman.service or foreman-proxy.service is started, it creates world-writable directory `/tmp/bundler/home`. Some users have reported that this triggers alarms in their security scans. Daemons that use `PrivateTmp=true` in their Systemd unit files create tmp directories at `/tmp/systemd-private-*-httpd.service-*/` instead with correct directory permissions.

As an example, PrivateTmp=true is the default setting for httpd shipped from RHEL-7 onwards [1].

[1] https://access.redhat.com/blogs/766093/posts/1976243

Related issues:

Related to Foreman - Feature #29417: Harden foreman.service using systemd fea...	**New**

Associated revisions

Revision d56290ba - 02/22/2021 04:26 PM - Evgeni Golov

Fixes #29960 - set PrivateTmp=true in foreman.service

Revision b260c03d - 02/23/2021 09:11 AM - Evgeni Golov

Refs #29960 - also set PrivateTmp=true for dynflow-sidekiq

History

#1 - 06/02/2020 07:29 AM - Lukas Zapletal

Older versions of bundler actually have a security issue with incorrect permissions on that directory allowing arbitrary code execution. I have reported this and it's been fixed :-)

#2 - 06/02/2020 07:29 AM - Lukas Zapletal

- Priority changed from Normal to High

- Triaged changed from No to Yes

#3 - 12/02/2020 12:18 PM - Ewoud Kohl van Wijngaarden

- Related to Feature #29417: Harden foreman.service using systemd features added

#4 - 02/22/2021 10:41 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Evgeni Golov

- Pull request https://github.com/theforeman/foreman/pull/8345 added

#5 - 02/22/2021 04:26 PM - The Foreman Bot

- Fixed in Releases 2.5.0 added

#6 - 02/22/2021 05:01 PM - Evgeni Golov

- Status changed from Ready For Testing to Closed

Applied in changeset foreman|d56290ba0e4133244f802de5a876af8b3b184df2.

#7 - 02/23/2021 08:27 AM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman/pull/8351 added

#8 - 02/24/2021 09:59 AM - Ondřej Ezr

- Target version set to 2.4.0

#9 - 02/24/2021 10:08 AM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman/pull/8356 added

#10 - 02/24/2021 10:33 AM - Ewoud Kohl van Wijngaarden

- Fixed in Releases 2.4.0 added

- Fixed in Releases deleted (2.5.0)