Packaging - Bug #30490
CVE-2020-14334 - unauthorized cache read on RPM-based installations through local user

07/24/2020 11:07 PM - Ondřej Ezr

Status: Closed
Priority: Normal
Assignee: Ondřej Ezr
Category: RPMs
Target version: 2.1.1

Pull request: https://github.com/theforeman/foreman-packaging/pull/5596,
https://github.com/theforeman/foreman-packaging/pull/5598,
https://github.com/theforeman/foreman-packaging/pull/5597

Triaged: Yes
Bugzilla link: 1858308

Description
Cache permissions allow unauthorized read

Associated revisions
Revision 5283f137 - 07/29/2020 12:24 PM - Ondřej Ezr
Fixes #30490 - CVE-2020-14334 world readable cache

History
#1 - 07/24/2020 11:13 PM - Ondřej Ezr
- File 0001-BZ-1858308-CVE-2020-14334-too-permissive-mode-for-ca.patch added

#2 - 07/28/2020 07:33 AM - Tomer Brisker
- Bugzilla link set to 1858308

#3 - 07/28/2020 07:34 AM - Tomer Brisker
- Subject changed from CVE-2020-14334 to CVE-2020-14334 - unauthorized cache read on RPM-based installations through local user

#4 - 07/28/2020 09:48 AM - Ewoud Kohl van Wijngaarden
This looks good. Perhaps it's Redmine formatting, but it looks like the whitespace might be a bit odd.

#5 - 07/29/2020 12:05 PM - Ondřej Ezr
- Private changed from Yes to No

Embargo is lifted.

#6 - 07/29/2020 12:08 PM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman-packaging/pull/5596 added

#7 - 07/29/2020 12:24 PM - The Foreman Bot
- Fixed in Releases 2.2.0 added
#8 - 07/29/2020 12:26 PM - Ondřej Ezr
Security page entry PR: [https://github.com/theforeman/theforeman.org/pull/1654](https://github.com/theforeman/theforeman.org/pull/1654)

#9 - 07/29/2020 12:29 PM - The Foreman Bot
- Pull request [https://github.com/theforeman/foreman-packaging/pull/5597](https://github.com/theforeman/foreman-packaging/pull/5597) added

#10 - 07/29/2020 12:31 PM - The Foreman Bot
- Pull request [https://github.com/theforeman/foreman-packaging/pull/5598](https://github.com/theforeman/foreman-packaging/pull/5598) added

#11 - 07/29/2020 01:01 PM - Ondřej Ezr
- Status changed from Ready For Testing to Closed

Applied in changeset [foreman-packaging|5283f1374294c5a62bb7f51140a6a2aaf10631b2](https://github.com/theforeman/foreman-packaging/pull/5598/commit/5283f1374294c5a62bb7f51140a6a2aaf10631b2).

#12 - 07/30/2020 09:38 AM - Ondřej Ezr
- Fixed in Releases 2.0.2, 2.1.1 added

**Files**

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-BZ-1858308-CVE-2020-14334-too-permissive-mode-for-ca.patch</td>
<td>12 KB</td>
<td>07/24/2020</td>
<td>Ondřej Ezr</td>
</tr>
</tbody>
</table>