Foreman - Bug #27103
update npm diff package due to security alert

06/23/2019 06:47 AM - Ohad Levy

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Ohad Levy</td>
</tr>
<tr>
<td>Category:</td>
<td>JavaScript stack</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>


Triaged: Yes

Fixed in Releases: 1.23.0

Bugzilla link:

Description
WS-2018-0590 More information high severity
Vulnerable versions: < 3.5.0
Patched version: 3.5.0
A vulnerability was found in diff before v3.5.0, the affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks.

This was fixed at https://github.com/kpdecker/jsdiff/commit/2aec4298639bf30fb88a00b356bf404d3551b8c0

Associated revisions
Revision 18649478 - 07/10/2019 03:28 PM - Ohad Levy
fixes #27103 - bump npm diff package version

Revision e8ec883f - 07/10/2019 04:25 PM - Ewoud Kohl van Wijngaarden
Refs #27103 - Allow diff 4.x in unidiff

Revision 7d385371 - 07/11/2019 05:54 AM - Ewoud Kohl van Wijngaarden
Refs #27103 - Pin diff to a major version
18649478cb128591738f97931f98632fd966d1f2 pinned it to a lower bound, but for our dependencies it's better to follow semver and not blindly allow new major versions.

History
#1 - 06/23/2019 06:50 AM - The Foreman Bot
- Assignee set to Ohad Levy
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/6853 added

#2 - 07/10/2019 03:29 PM - Ewoud Kohl van Wijngaarden
- Triaged changed from No to Yes
- Fixed in Releases 1.23.0 added

03/25/2022
#3 - 07/10/2019 04:01 PM - Ohad Levy
- Status changed from Ready For Testing to Closed
  
  Applied in changeset 18649478cb128591738f97931f98632fd966df152.

#4 - 07/10/2019 04:26 PM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman-packaging/pull/3902 added

#5 - 07/10/2019 04:59 PM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/6889 added

#6 - 08/05/2019 01:41 PM - Tomer Brisker
- Category changed from Security to JavaScript stack