Discovery - Bug #14140

Arbitrary Ruby code execution via Discovery setting

03/10/2016 08:49 AM - Lukas Zapletal

<table>
<thead>
<tr>
<th>Status</th>
<th>Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Alon Goldboim</td>
</tr>
<tr>
<td>Category</td>
<td>Image</td>
</tr>
<tr>
<td>Target version</td>
<td>Discovery Plugin 5.0.2</td>
</tr>
<tr>
<td>Difficulty</td>
<td>trivial</td>
</tr>
<tr>
<td>Triaged</td>
<td>No</td>
</tr>
</tbody>
</table>

Pull request: https://github.com/theforeman/foreman_discovery/pull/260

Description

We have couple of evals during review of new Discovery Show page:


You can run arbitrary Ruby code by entering it on the About - Settings - Discovery and then visiting a discovered host detail page where it gets rendered.

Associated revisions

Revision 7b8ac717 - 03/10/2016 11:12 AM - Alon Goldboim
Fixes #14099, #14140 - removed the use of eval, typos

History

#1 - 03/10/2016 08:49 AM - Lukas Zapletal
- Description updated

#2 - 03/10/2016 11:00 AM - Lukas Zapletal
- Status changed from New to Ready For Testing
- Assignee changed from Lukas Zapletal to Alon Goldboim
- Pull request https://github.com/theforeman/foreman_discovery/pull/260 added

#3 - 03/10/2016 11:05 AM - Dominic Cleal
- Private changed from Yes to No

Marking as public as it's been referenced in the associated pull request.

Lukas has also reported it to foreman-security and since this only affects the version of Discovery that's used with a release candidate version of Foreman, no CVE will be assigned as it's generally pre-release. The issue should be resolved in time for 1.11.0's release and it should be documented on http://theforeman.org/security.html.

#4 - 03/10/2016 11:13 AM - Lukas Zapletal
- Status changed from Ready For Testing to Resolved

Merged into develop and 5.0 series, bugfix release by EOBW.