### Facts search vulnerable to SQL injection

11/12/2015 11:04 AM - Dominic Cleal

<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>Dominic Cleal</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.10.0</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman/pull/2908">https://github.com/theforeman/foreman/pull/2908</a></td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td></td>
</tr>
<tr>
<td>Found in Releases:</td>
<td></td>
</tr>
</tbody>
</table>

#### Description

The search for facts and also hosts by facts is vulnerable to SQL injection by breaking out of quotes in either the fact name or the fact value.

**Hosts search term:** facts.bobby'tables = test

```sql
SQLite3::SQLException: near "tables": syntax error: SELECT "hosts".* FROM "hosts" INNER JOIN fact_values fact_values_66 ON (hosts.id = fact_values_66.host_id) INNER JOIN fact_names fact_names_66 ON (fact_names_66.id = fact_values_66.fact_name_id) WHERE "hosts"."type" IN ('Host::Managed') AND ((fact_names_66.name = 'bobby\'tables\' AND fact_values_66.value = 'test')) ORDER BY "hosts"."name" ASC LIMIT 40 OFFSET 0
```

**Hosts search term:** facts.test = a'b

```sql
SQLite3::SQLException: near "b": syntax error: SELECT "hosts".* FROM "hosts" INNER JOIN fact_values fact_values_62 ON (hosts.id = fact_values_62.host_id) INNER JOIN fact_names fact_names_62 ON (fact_names_62.id = fact_values_62.fact_name_id) WHERE "hosts"."type" IN ('Host::Managed') AND ((fact_names_62.name = 'test' AND fact_values_62.value = 'a\'b\') ORDER BY "hosts"."name" ASC LIMIT 40 OFFSET 0
```

The host search by facts mechanism was extended in [#11150](https://github.com/theforeman/foreman/pull/2908) to support integer comparisons, and in the process the custom SQL that was added doesn't escape non-integer values when it constructs the query.

This was added in Foreman 1.10.0, so only the current release candidates are affected.

CVE identifier requested.

#### Related issues:

- Related to Foreman - Feature #11150: Allow searching of facts as types other ...

  - Closed
  - 07/19/2015

#### Associated revisions

- **Revision b08ec33d** - 11/13/2015 05:47 AM - Dominic Cleal
  
  fixes #12458 - escape values in fact searches to prevent SQL injection

- **Revision 72eac09d** - 11/16/2015 09:30 AM - Dominic Cleal
  
  fixes #12458 - escape values in fact searches to prevent SQL injection
History

#1 - 11/12/2015 11:04 AM - Dominic Cleal
- Related to Feature #11150: Allow searching of facts as types other than string added

#2 - 11/12/2015 11:42 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/2908 added

#3 - 11/13/2015 03:14 AM - Dominic Cleal

CVE identifier requested.

This won't be assigned as the software is pre-release.

#4 - 11/13/2015 06:01 AM - Dominic Cleal
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset b08ec33dbb1e12db65bc0bde755e657a940531c1.