A user who has no roles or permissions can still view task’s details both through the web UI and through API, if the user knows the UUID of the task. I know UUIDs are tough to guess, but...

This was introduced in foreman-tasks@79a0e2cb5 [1], before this commit tasks were looked up through find_resource which performed authorization checks. After this change, permissions are bypassed.

Steps to reproduce:
1) Have foreman with foreman-tasks >= 0.7.8
2) Trigger a couple of tasks
3) Create a user, assign no roles to the user
4.1) As the user, visit $foreman/foreman_tasks/tasks/$UUID, where $UUID is UUID of a task from 2)
4.2) As the user, visit $foreman/foreman_tasks/tasks/$UUID/sub_tasks, where $UUID is UUID of a task from 2) which has sub tasks
4.3) As the user, perform get request against $foreman/foreman_tasks/api/tasks/$UUID

Actual result:
In the UI, task details are shown. For task with sub tasks, sub tasks are shown on an index-like page.
In the API, details are provided.

Expected result:
In the UI, permission denied page is shown.
In the API, the request fails with either 403 or 404.

```bash
# curl -u user:changeme -k https://localhost/foreman_tasks/api/tasks/f4211c3e-467f-405e-a70c-980d6c4d4e0f 2>/dev/null | ruby -e "require 'json'; puts JSON.pretty_generate(JSON.parse(STDIN.read))"
{
  "id": "f4211c3e-467f-405e-a70c-980d6c4d4e0f",
  "label": "Actions::RemoteExecution::RunHostJob",
  "pending": false,
  "action": "Remote action: Run sleep 60 on helpful-snipe.lxd",
  "username": "admin",
  "started_at": "2019-07-10 12:21:44 UTC",
  "ended_at": "2019-07-10 12:22:50 UTC",
  "state": "stopped",
  "result": "success",
  "progress": 1.0,
  "input": {
    "host": {
      "id": 1,
      "name": "helpful-snipe.lxd"
    },
    "job_category": "Commands",
    "description": "Run sleep 60",
    "delegated_action_id": 2,
    "locale": "en",
    "current_request_id": null,
    "current_timezone": "Europe/Prague",
  }
}
```

1/2
"current_user_id": 4,
"current_organization_id": 1,
"current_location_id": 2
},
"output": {
},
"humanized": {
"action": "Remote action:",
"input": "Run sleep 60 on helpful-snipe.lxd",
"output": "Exit status: 0",
"errors": [
]
},
"cli_example": null

[1] - https://github.com/theforeman/foreman-tasks/pull/151/commits/79a0e2cb52fbf872863a3a176e5b1d9a09fc984d

Associated revisions
Revision 3104a46c - 07/15/2019 11:33 AM - Adam Růžička
Fixes #27275 - Fix permission bypasses in controllers

History
#1 - 07/11/2019 01:02 PM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman-tasks/pull/434 added

#2 - 07/11/2019 01:15 PM - Tomer Brisker
- Subject changed from Authorization bypasses when accessing task details to CVE-2019-1019 Authorization bypasses when accessing task details

#3 - 07/11/2019 01:16 PM - Adam Ruzicka
- Bugzilla link set to 1729149

#4 - 07/11/2019 01:24 PM - Tomer Brisker
- Subject changed from CVE-2019-1019 Authorization bypasses when accessing task details to CVE-2019-10198 Authorization bypasses when accessing task details

#5 - 07/15/2019 12:01 PM - Anonymous
- Status changed from Ready For Testing to Closed

Applied in changeset 3104a46cf669ae62f9034e9547cb93cc03384cd9.