New issue

Jump to bottom

XEN Orchestra privilege escalation via websockets #5712

Open r3naissance opened this issue on Apr 5, 2021 · 2 comments

Assignees

r3naissance commented on Apr 5, 2021 • edited by julien-f

Context

- **XO origin**: XO Appliance
- **Versions**:
  - Node: 14.15.0
  - xo-web: 5.76.0
  - xo-server: 5.73.0

Validated still vulnerable on version:

- **Versions**:
  - Node: 14.17.3
  - xo-web: 5.80.0
  - xo-server: 5.84.0

Expected behavior

Permissions enforcement through websockets is not thoroughly checked and can lead to an unprivileged 'user' to obtain data only accessible by 'admin'. VMs, Backups, Audit, Users, Groups, etc.

Current behavior

The websockets that control the application API are allowing access to certain elements based purely on the response (which can be manipulated). This would be similar to an ecommerce application taking the price of a shopping cart from the DOM (can be manipulated by the user) and starting the checkout process using this value).

In this POC, the method 'resourceSet.getAll' [Figure 1] responds with `"permission":"none"` [Figure 2]. If an attacker changes the value of `'none'` to `'admin'` [Figure 3], the API opens up with further data and UI points [Figure 4]. This change in permission level persists through other API calls until the `resourceSet.getAll` method calls for permissions again (which should respond with "none") unless the attacker changes it back to admin. Interestingly, the API limits some methods, returning with 'not enough permissions' but shows the user has 'admin' permissions [Figure 5].

```
{"id":-9007199254740907,"jsonrpc":"2.0","method":"resourceSet.getAll"}
```


WebSockets message from http://192.168.85.33/api/

Forward | Drop | Intercept is on | Action | Open Browser

\n | Actions


```
{"id":-9007199254740908,"jsonrpc":"2.0","result":{"id":"9253d680-c83a-4092-9356-9d47386b586d","email":"test","groups":[],"permission":"none","preferences":{}}}
```


'test' user

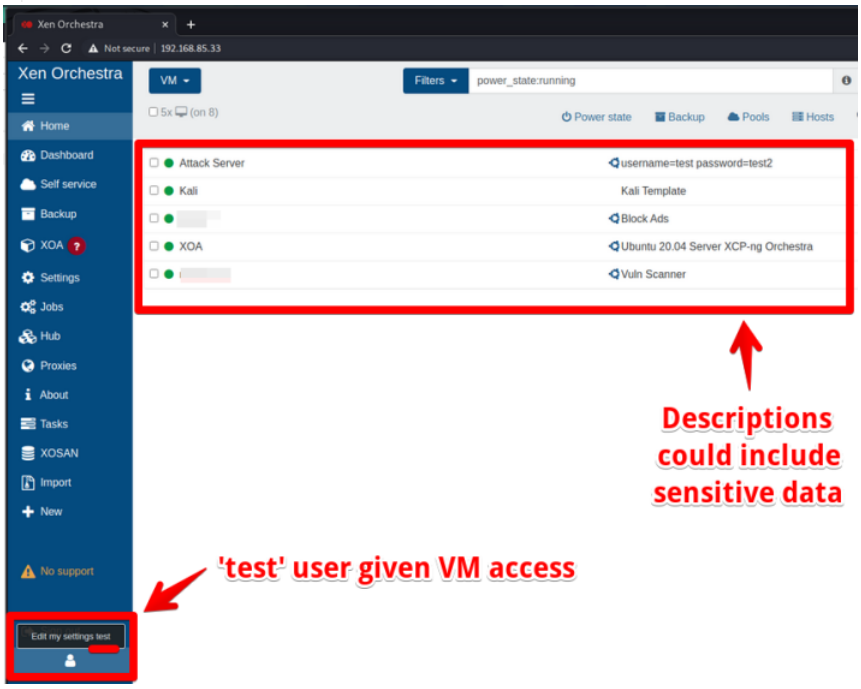
WebSockets message from http://192.168.85.33/api/

Forward | Drop | Intercept is on | Action | Open Browser

Change to admin

\n | Actions


```
{"id":-9007199254740908,"jsonrpc":"2.0","result":{"id":"9253d680-c83a-4092-9356-9d47386b586d","email":"test","groups":[],"permission":"admin","preferences":{}}}
```

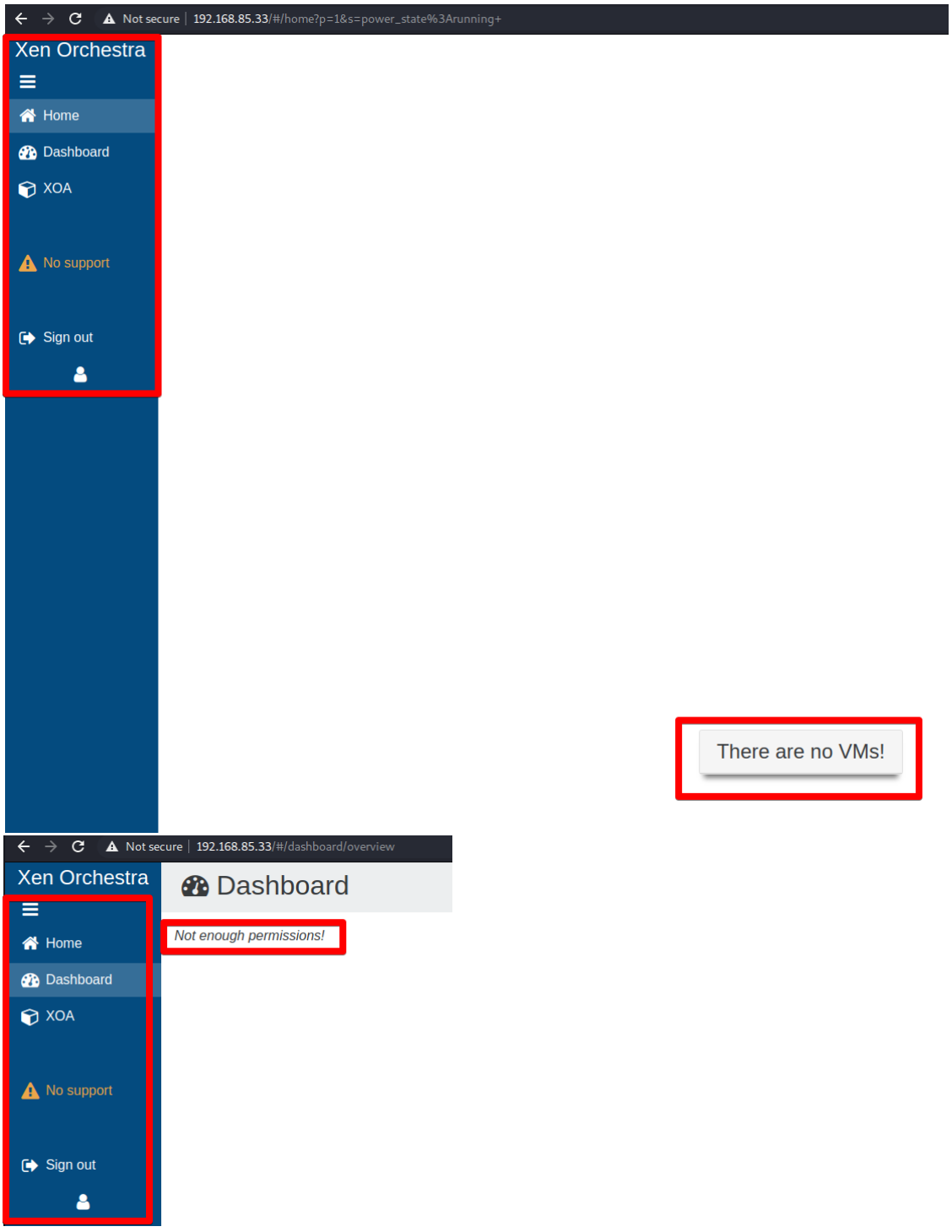



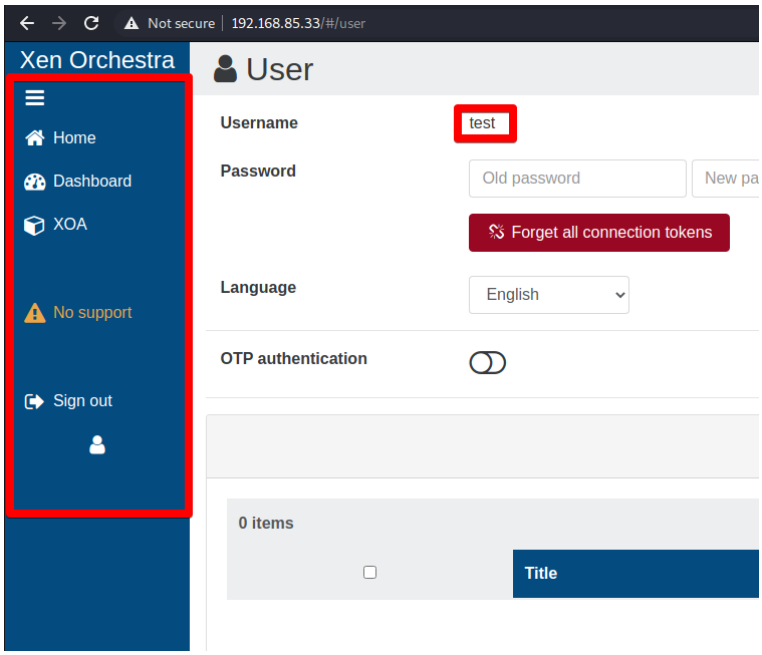
WebSockets message from http://192.168.85.33/api/

Forward | Drop | Intercept is on | Action | Open Browser

\n | Actions


```
{"error":{"message":"not enough permissions","code":2,"data":{"permission":"admin","object":{}}},"id":-9007199254740869,"jsonrpc":"2.0"}
```


Not secure | 192.168.85.33/#/home?p=1&s=power_state%3Arunning+
Xen Orchestra
Home
Dashboard
XOA
No support
Sign out
There are no VMs!
Not secure | 192.168.85.33/#/dashboard/overview
Xen Orchestra
Dashboard
Not enough permissions!
Home
Dashboard
XOA
No support
Sign out



julien-f self-assigned this on Apr 6, 2021

julien-f commented on Jul 13, 2021 • edited by olivierlambert — Member

Hello,

Sorry for the delay.

From what I understand, it's not a new issue and it's not a privilege escalation per se: API users can see all objects regardless of their permissions, the filtering is only done by the UI at the moment, but they cannot do any actions on objects they don't have the right to.

This is something we are actively working on fixing for the next major iteration of XO (v6).

Please see #502 for more information.

julien-f commented on Jul 13, 2021 — Member

Just to be clear, this issue should only impacts XAPI objects (VMs, hosts, pools, etc).

Other info (users, groups, backup jobs, etc) should not be accessible.

Assignees

julien-f

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants