Foreman - Bug #23028

CVE-2018-1096: SQL injection in dashboard controller

03/27/2018 01:28 PM - Tomer Brisker

Status:	Closed		
Priority:	High		
Assignee:	Tomer Brisker		
Category:	Security		
Target version:	1.16.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.9.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/5363, https://github.com/theforeman/foreman/pull/5364, https://github.com/theforeman/foreman/pull/5365		

Description

Widget id is not properly escaped for save_positions action on the dashboard, leading to SQL injection possibility.
This only allows injecting conditions to the select conditions, as it is a prepared query it does not allow executing additional commands.
It is only available to authenticated users.

This issue was reported by Martin Povolný from Red Hat.

Related issues:

Related to Foreman - Refactor #8106: Save dashboard widgets in DB to increase...	**Closed**	**10/26/2014**

Associated revisions

Revision 274665e2 - 03/27/2018 04:22 PM - Martin Povolny

Fixes #23028 - Properly escape params passed to where (CVE-2018-1096) (#5363)

History

#1 - 03/27/2018 02:01 PM - Tomer Brisker

- Description updated

#2 - 03/27/2018 03:03 PM - Tomer Brisker

- Related to Refactor #8106: Save dashboard widgets in DB to increase flexibility added

#3 - 03/27/2018 03:03 PM - Tomer Brisker

- Subject changed from SQL injection in dashboard controller to CVE-2018-1096: SQL injection in dashboard controller

- Private changed from Yes to No

#4 - 03/27/2018 03:05 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/5363 added

#5 - 03/27/2018 04:22 PM - Tomer Brisker

- translation missing: en.field_release set to 332

#6 - 03/27/2018 04:25 PM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman/pull/5364 added

#7 - 03/27/2018 04:28 PM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman/pull/5365 added

#8 - 03/27/2018 05:01 PM - Martin Povolny

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 274665e24373de670a9107d4565c10ec41dd5f65.