Foreman - Issues

#	Tracker	Status	Priority	Subject	Author	Assignee	Updated	Category	Target version
36644	Bug	Closed	Normal	Open Redirect weakness in links_controller.rb	Evgeni Golov	Evgeni Golov	09/11/2023 10:32 AM	Security	
36219	Refactor	Closed	Normal	use YAML.safe_load instead of YAML.load	Ron Lavi	Ron Lavi	09/12/2023 08:36 AM	Security	
36097	Bug	Closed	Normal	User without view_provisioning_templates permission is able to see the rendered template	Bernhard Suttner	Bernhard Suttner	05/25/2023 11:52 AM	Security	
34573	Bug	Closed	Normal	Settings defined by DSL are not properly encrypted	Ondřej Ezr	Ondřej Ezr	03/14/2022 10:42 PM	Security	3.1.3
33417	Bug	Closed	Normal	The login page exposes version of the foreman	Lukas Zapletal	Anna Vítová	12/14/2021 08:01 AM	Security	
31937	Bug	Closed	Normal	CVE-2021-20256 foreman: BMC controller credential leak via API	Evgeni Golov	Evgeni Golov	03/01/2021 02:54 PM	Security	2.5.0
30739	Bug	Closed	Normal	CVE-2020-14380: Users can gain elevated rights when logging in with SSO accounts	Tomer Brisker	Rahul Bajaj	09/10/2020 05:12 AM	Security	2.1.3
28861	Bug	Closed	Normal	SSH key cannot be added when FIPS enabled	Leos Stejskal	Leos Stejskal	02/17/2020 12:15 PM	Security	
28458	Bug	Closed	Normal	remove gravater from img_src secure header	Tomer Brisker	Tomer Brisker	12/10/2019 04:01 PM	Security	
25451	Bug	Closed	Normal	Certificate extraction service can't handle joined lines	Ewoud Kohl van Wijngaarden	Ewoud Kohl van Wijngaarden	01/14/2019 05:20 PM	Security	1.21.0
25191	Bug	Resolved	High	Canned admin role gives non-admin users access to settings	Michael Johnson		10/12/2018 07:10 PM	Security	
25169	Bug	Closed	Normal	CVE-2018-14664 - Persisted XSS on all pages that use breadcrumbs	Marek Hulán	Amir Fefer	11/25/2018 08:19 AM	Security	1.18.3
24807	Bug	Closed	High	CVE-2018-16861 - toast notification sends strings through as HTML	Chris Duryee	Avi Sharvit	11/25/2018 08:22 AM	Security	
23621	Bug	Closed	High	fips mode breaks ESXi deployment	Jeff Sparrow	Timo Goebel	07/10/2018 09:58 AM	Security	1.17.2
23444	Refactor	Closed	Low	update secure_headers to 5.x	Anonymous		06/05/2018 06:48 AM	Security	
23128	Bug	Resolved	Normal	Deface uses MD5 and doesn't work in FIPS-enable environment	Ivan Necas		10/15/2018 11:24 AM	Security	
23028	Bug	Closed	High	CVE-2018-1096: SQL injection in dashboard controller	Tomer Brisker	Tomer Brisker	07/10/2018 09:58 AM	Security	1.16.1
22778	Refactor	Closed	Normal	Allow admin to opt-out from the Brute-force attack protection	roman plevka	Marek Hulán	09/26/2018 07:43 PM	Security	1.19.0
22546	Bug	Closed	Urgent	CVE-2018-1097: curl api to change power state on ovirt compute_resource exposes credentials	Steve D	Ori Rabin	11/11/2019 07:06 PM	Security	1.16.1
22119	Feature	Closed	Normal	Replace MD5 hashes with SHA	Anonymous	Ivan Necas	10/03/2018 09:01 AM	Security	
21519	Bug	Closed	Normal	CVE-2017-15100: Stored XSS in fact name or value	Tomer Brisker	Tomer Brisker	07/10/2018 09:57 AM	Security	1.16.0
20963	Bug	Closed	Low	CVE-2017-7535: stored XSS in the manage organization page	Tomer Brisker	Tomer Brisker	07/10/2018 09:57 AM	Security	1.16.0
20271	Bug	Closed	High	Safe mode rendering does not correctly prevent using symbol to proc calls	Tomer Brisker	Tomer Brisker	07/10/2018 09:54 AM	Security	1.15.3
19612	Bug	Closed	Normal	CVE-2017-7505: User scoped in organization with permissions for user management can manage administrators that are not assigned to any organization	Marek Hulán	Marek Hulán	07/10/2018 09:54 AM	Security	1.15.1

#	Tracker	Status	Priority	Subject	Author	Assignee	Updated	Category	Target version
19044	Bug	Rejected	Normal	Do not send username into logs with every request	Lukas Zapletal	Lukas Zapletal	04/10/2017 07:20 AM	Security	
18735	Bug	Closed	Normal	Encryptable unit tests fail under Ruby 2.4: key must be 32 bytes	Dominic Cleal	Dominic Cleal	07/10/2018 09:54 AM	Security	1.15.0
17854	Bug	Duplicate	Normal	When user is deleted and they still have an active session in browser, they are not logged out	Tomer Brisker		12/27/2016 06:57 AM	Security	
17516	Bug	Closed	Normal	Update jquery to 2.2.4 to fix XSS	Daniel Lobato Garcia	Daniel Lobato Garcia	07/10/2018 09:54 AM	Security	1.15.0
17195	Bug	Closed	Normal	CVE-2016-8634 - Organization/location wizard may run stored XSS through alert	Dominic Cleal	Tomer Brisker	07/10/2018 09:52 AM	Security	1.14.0
16982	Bug	Closed	Normal	CVE-2016-7078 - User with no organizations or locations can see all resources	Daniel Lobato Garcia	Daniel Lobato Garcia	07/10/2018 09:54 AM	Security	1.15.0
16971	Bug	Closed	Normal	CVE-2016-7077 - Association lists (for < 6 items) shown without authorization/filters	Marek Hulán	Marek Hulán	07/10/2018 09:52 AM	Security	1.14.0
16024	Bug	Closed	Normal	Foreman form helpers do not escape JS when rendering label	Marek Hulán	Marek Hulán	07/10/2018 09:52 AM	Security	1.12.2
16022	Bug	Closed	Normal	CVE-2016-6320 - Network interface device identifiers may contain stored XSS on host form	Dominic Cleal	Tomer Brisker	07/10/2018 09:52 AM	Security	1.12.2
16020	Bug	Closed	Normal	Reflective XSS in Smart Variables	Tomer Brisker	Tomer Brisker	07/10/2018 09:52 AM	Security	1.12.2
15490	Bug	Closed	Normal	CVE-2016-4995 - view_hosts permissions/filters not checked for provisioning template previews	Dominic Cleal	Lukas Zapletal	07/10/2018 09:51 AM	Security	1.11.4
15268	Bug	Closed	High	CVE-2016-4475 - API and UI org/locations actions not limited to user's associated orgs/locations	Dominic Cleal	Marek Hulán	07/10/2018 09:51 AM	Security	1.11.4
15182	Bug	Closed	Normal	CVE-2016-4451 - Privileges escalation through Organization and Locations API	Marek Hulán	Marek Hulán	07/10/2018 09:51 AM	Security	1.11.3
14635	Bug	Closed	High	CVE-2016-3693 - `inspect` in a provisioning template exposes sensitive controller information	Dominic Cleal	Ivan Necas	07/10/2018 09:51 AM	Security	1.11.1
13828	Bug	Closed	Normal	CVE-2016-2100 - unprivileged user can see private bookmarks in Administer -> Bookmarks	Ohad Levy	Tom Caspy	07/10/2018 09:51 AM	Security	1.10.3
13817	Bug	Closed	Normal	ENC smart proxy validation fails	Matthew Ceroni	Matthew Ceroni	07/10/2018 09:49 AM	Security	1.11.0
12698	Bug	Closed	Normal	Insufficient URL validation for smart proxy and medium	Daniel Lobato Garcia	Daniel Lobato Garcia	07/10/2018 09:49 AM	Security	1.11.0
12611	Bug	Closed	Normal	CVE-2015-7518 - Smart class parameters/variables shown on host edit allows stored XSS in description	Dominic Cleal	Tomer Brisker	07/10/2018 09:50 AM	Security	1.10.0
12458	Bug	Closed	Normal	Facts search vulnerable to SQL injection	Dominic Cleal	Dominic Cleal	07/10/2018 09:50 AM	Security	1.10.0
11859	Bug	Closed	Normal	CVE-2015-5282 - Parameter hide/show checkbox allows stored XSS during textbox change	Dominic Cleal	Shlomi Zadok	07/10/2018 09:50 AM	Security	1.10.0
11816	Bug	Closed	Normal	Remove whitelist_attributes as it's deprecated	Daniel Lobato Garcia	Daniel Lobato Garcia	07/10/2018 09:50 AM	Security	1.10.0
11579	Bug	Closed	High	CVE-2015-5233 - reports show/destroy not restricted by host authorization	Dominic Cleal	Daniel Lobato Garcia	07/10/2018 09:49 AM	Security	1.8.4

#	Tracker	Status	Priority	Subject	Author	Assignee	Updated	Category	Target version
11352	Bug	Rejected	Normal	Foreman 1.7.5 CVE-2015-3155 - The _session_id cookie is issued without the Secure flag	Brian Lee		05/20/2017 06:40 AM	Security	
11119	Bug	Closed	Normal	CVE-2015-5152 - API permits HTTP requests when require_ssl is enabled	Dominic Cleal		07/10/2018 09:48 AM	Security	1.9.0
10510	Bug	Closed	High	"Invalid authenticity token" after login	Anonymous	Dominic Cleal	07/10/2018 09:48 AM	Security	1.8.1
10289	Bug	Closed	Normal	Change default root password hash function from MD5 to SHA256	Anonymous		07/10/2018 09:48 AM	Security	1.9.0
10275	Bug	Closed	Normal	CVE-2015-3155 - The _session_id cookie is issued without the Secure flag	Ori Rabin	Shlomi Zadok	07/10/2018 09:48 AM	Security	1.8.1
10263	Feature	Closed	Normal	Encrypt LDAP password in database	Daniel Lobato Garcia	Daniel Lobato Garcia	07/10/2018 09:48 AM	Security	1.9.0
9775	Bug	Closed	High	CR encryption key not loaded before it's checked, encryption is disabled	Dominic Cleal	Dominic Cleal	07/10/2018 09:47 AM	Security	1.8.0
8091	Bug	Closed	Normal	Secure websockets connection denied by secure headers	Daniel Lobato Garcia	Daniel Lobato Garcia	07/10/2018 09:46 AM	Security	1.7.0
7805	Feature	Closed	Normal	Add several security related HTTP headers - security hardening.	Jan Rusnacko	Jan Rusnacko	07/10/2018 09:46 AM	Security	1.7.0
7736	Bug	Rejected	Normal	Change to prevent unauthenticated requests for CSRF modified login behaviour as well	Jan Pazdziora		09/29/2014 11:07 AM	Security	
7731	Bug	Duplicate	Normal	Default OS root password hash algorithm should be SHA-2	Dominic Cleal		04/28/2015 07:39 AM	Security	
7657	Bug	Closed	Normal	Remove default OAuth credentials	Dominic Cleal	Shlomi Zadok	07/10/2018 09:46 AM	Security	1.7.0
7483	Bug	Closed	Normal	CVE-2014-3653 - Provisioning Templates Preview mode strips out text like <<FOO	Aaron Stone	Aaron Stone	07/10/2018 09:45 AM	Security	1.6.1
6999	Bug	Closed	Normal	CVE-2014-3590 - User logout susceptible to CSRF attack	Dominic Cleal	Daniel Lobato Garcia	07/10/2018 09:46 AM	Security	1.6.1
6580	Bug	Closed	High	CVE-2014-3531 - XSS in operating system name / description	Dominic Cleal	Daniel Lobato Garcia	07/10/2018 09:45 AM	Security	1.5.2
6149	Bug	Closed	Urgent	CVE-2014-3492 - XSS in host YAML view	Dominic Cleal	Lukas Zapletal	07/10/2018 12:50 PM	Security	1.4.5
5926	Feature	Closed	Normal	Hide global parameter values	Marek Hulán	Marek Hulán	07/10/2018 09:46 AM	Security	1.7.0
5881	Bug	Closed	High	CVE-2014-3491 - XSS from create/update/destroy notification boxes	Dominic Cleal	Joseph Magen	07/10/2018 12:50 PM	Security	1.4.5
5471	Bug	Closed	High	CVE-2014-0208 - Stored XSS inside search auto-complete key names via parameters	Dominic Cleal	Amos Benari	07/10/2018 09:45 AM	Security	1.4.4
5463	Bug	Duplicate	Normal	No authentication required for /unattended/provision?hostname=HOSTNAME	Dylan Charleston		04/28/2014 08:04 AM	Security	
4555	Bug	Closed	Normal	Foreman doesn't validate peer certificate when connecting to ovirt	Amos Benari	Amos Benari	07/10/2018 09:45 AM	Security	1.5.0
4457	Bug	Closed	Urgent	CVE-2014-0090 - Session fixation, new session IDs are not generated on login	Dominic Cleal	Dominic Cleal	07/10/2018 09:44 AM	Security	1.4.2

#	Tracker	Status	Priority	Subject	Author	Assignee	Updated	Category	Target version
4456	Bug	Closed	Urgent	CVE-2014-0089 - Stored Cross Site Scripting (XSS) on 500 error page	Dominic Cleal	Joseph Magen	07/10/2018 09:44 AM	Security	1.4.2
4240	Feature	Duplicate	Low	[RFE] Cookies should only be sent up over https	Bryan Kearney		10/09/2015 09:23 AM	Security	
4239	Feature	Rejected	Normal	Disable password Auto-complete	Bryan Kearney		02/11/2014 08:53 AM	Security	
4238	Feature	Closed	Normal	Protection from Brute Force Password Attacks	Bryan Kearney	Tomer Brisker	07/10/2018 09:56 AM	Security	1.17.0
4167	Bug	Closed	Normal	Password length verification doesn't work	Stephen Benjamin	Stephen Benjamin	07/10/2018 09:45 AM	Security	1.5.0
3978	Bug	Rejected	Urgent	Ruby heap overflow in floating point parsing (CVE-2013-4164)	Lukas Zapletal		01/09/2014 09:43 AM	Security	
3976	Feature	Closed	Normal	Need Read-Only user Role pre-defined and available post installation	Mike McCune	Daniel Lobato Garcia	07/10/2018 09:46 AM	Security	1.7.0
3725	Feature	Closed	Urgent	Make default root password more explicit and configurable at install time	Dominic Cleal	Stephen Benjamin	07/10/2018 09:45 AM	Security	1.5.0
3601	Feature	Closed	Normal	Use secure websockets for console access	Ewoud Kohl van Wijngaarden	Daniel Lobato Garcia	07/10/2018 09:46 AM	Security	1.6.0
3511	Feature	Resolved	Normal	As a security person, I would like Foreman to run in FIPS mode	Anonymous		10/09/2018 05:22 PM	Security	
3160	Bug	Closed	Urgent	CVE-2013-4386 - SQL injection in host and host group lookup_value overrides/matcher associations	Dominic Cleal	Dominic Cleal	10/07/2013 12:21 PM	Security	1.2.3
2863	Bug	Closed	Normal	CVE-2013-4182 - Privileges escalation via API	Marek Hulán	Marek Hulán	09/03/2013 10:31 AM	Security	1.2.2
2860	Bug	Closed	Normal	CVE-2013-4180 - Potential DoS in HostsController	Marek Hulán	Marek Hulán	09/03/2013 10:31 AM	Security	1.2.2
2631	Bug	Closed	Immediate	Remote code execution in Foreman via bookmark controller name	Dominic Cleal	Joseph Magen	06/07/2013 06:17 AM	Security	1.2.0
2630	Bug	Closed	Urgent	Users with create/edit user permissions can escalate to admin	Dominic Cleal	Marek Hulán	06/07/2013 06:17 AM	Security	1.2.0
2127	Feature	Closed	Normal	Support newer hash schemes for root passwords	Dominic Cleal		07/10/2018 09:46 AM	Security	1.7.0
2125	Feature	Closed	Normal	SELinux support	Ewoud Kohl van Wijngaarden	Sam Kottler	03/25/2013 09:06 AM	Security	1.2.0
2121	Bug	Closed	Immediate	Unauthenticated YAML fact and reports importers can be exploited	Dominic Cleal	Dominic Cleal	02/07/2013 03:03 AM	Security	1.1
2069	Bug	Closed	High	(encrypted) root passwords are world readable	Andreas Rogge	Dominic Cleal	02/07/2013 03:03 AM	Security	1.1
1519	Bug	Duplicate	High	rails security problem	Florian Koch		09/18/2014 03:19 AM	Security	
1329	Feature	Closed	Normal	Encrypt BMC password	Corey Osman	Amir Fefer	07/10/2018 09:52 AM	Security	1.12.0
1328	Feature	Duplicate	Normal	Encrypt Hypervisor password	Corey Osman		07/30/2013 03:08 AM	Security	