Foreman - Bug #32753

CVE-2021-3584: Remote code execution through Sendmail configuration

06/08/2021 09:59 AM - Lukas Zapletal

Status:	Closed		
Priority:	High		
Assignee:	Lukas Zapletal		
Category:	Settings		
Target version:	2.5.1		
Difficulty:	easy	**Fixed in Releases:**	2.4.1, 2.5.1, 3.0.0
Triaged:	Yes	**Found in Releases:**	1.15.0
Bugzilla link:	1968443	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/8599		

Description

Sendmail location and arguments, available via Administer - Settings,
both accept arbitrary strings and pass them into shell.
By default, only Foreman super administrator can access settings.

Mitigation: Verify the both settings and remove edit_settings
permissions to all roles and users until fixed. Alternatively, create
settings named sendmail_location and sendmail_arguments in settings.yaml
file to override the UI and make the values read-only.

Solution: Limit the possible values for location to just expected paths.
Use shellescaping for arguments as there is currently no way to pass
arguments to the 'mail' gem in a safely manner.

Related issues:

Related to Installer - Bug #32827: Set sendmail location and arguments via pu...	**Closed**

Associated revisions

Revision c83d799e - 06/22/2021 11:15 AM - Lukas Zapletal

Fixes #32753 - Remote code execution through Sendmail

CVE-2021-3584: Sendmail location and arguments, available via Administer
- Settings, both accept arbitrary strings and pass them into shell.
By default, only Foreman super administrator can access settings.

Mitigation: Verify the both settings and remove edit_settings
permissions to all roles and users until fixed. Alternatively, create
settings named sendmail_location and sendmail_arguments in settings.yaml
file to override the UI and make the values read-only.

Solution: Limit the possible values for location to just expected paths.
Use shellescaping for arguments as there is currently no way to pass
arguments to the 'mail' gem in a safely manner.

History

#1 - 06/09/2021 06:57 AM - Lukas Zapletal

- File sendmail-32753-a.patch added

- Description updated

#2 - 06/10/2021 01:32 PM - Lukas Zapletal

- File sendmail-32753-b.patch added

#3 - 06/17/2021 07:02 AM - Lukas Zapletal

- Private changed from Yes to No

- Pull request https://github.com/theforeman/foreman/pull/8599 added

Embargo lifted.

#4 - 06/17/2021 07:03 AM - The Foreman Bot

- Status changed from New to Ready For Testing

#5 - 06/17/2021 11:08 AM - Ewoud Kohl van Wijngaarden

- Category deleted (Security)

- Assignee deleted (Lukas Zapletal)

- Target version deleted (2.5.1)

- Found in Releases 1.15.0 added

#6 - 06/17/2021 11:09 AM - Ewoud Kohl van Wijngaarden

- Category set to Settings

- Assignee set to Lukas Zapletal

- Target version set to 2.5.1

That's not what I intended to do ...

#7 - 06/22/2021 11:15 AM - The Foreman Bot

- Fixed in Releases 3.0.0 added

#8 - 06/22/2021 11:18 AM - Tomer Brisker

- Fixed in Releases 2.4.1, 2.5.1 added

#9 - 06/22/2021 11:29 AM - Ewoud Kohl van Wijngaarden

- Related to Bug #32827: Set sendmail location and arguments via puppet/installer added

#10 - 06/22/2021 12:08 PM - Lukas Zapletal

- Status changed from Ready For Testing to Closed

Applied in changeset foreman|c83d799eee3d10d27d9e7d5900232b9e979e4a21.

Files

sendmail-32753-a.patch	3.38 KB	06/09/2021	Lukas Zapletal
sendmail-32753-b.patch	4.52 KB	06/10/2021	Lukas Zapletal