Installer - Bug #36760

CVE-2023-4886: World readable tomcat server.xml contains passwords

09/20/2023 09:21 AM - Ewoud Kohl van Wijngaarden

Status:	Closed		
Priority:	Normal		
Assignee:	Ewoud Kohl van Wijngaarden		
Category:	Foreman modules		
Target version:	3.8.0		
Difficulty:		**Fixed in Releases:**	3.8.0
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-candlepin/pull/242, https://github.com/theforeman/foreman-installer/pull/886, https://github.com/theforeman/foreman-installer/pull/887, https://github.com/theforeman/foreman-installer/pull/890		

Description

The file /etc/tomcat/server.xml contains passwords and is world readable. The actual keystore is limited by file permissions, but server.xml should also be limited.

Associated revisions

Revision 0f0595d7 - 10/05/2023 01:46 PM - Ewoud Kohl van Wijngaarden

Fixes #36760 - Limit access to server.xml

Prior to this the file was world readable, even though it contained
passwords for the keystore. That keystore was limited to just the
correct group, so it's not directly exploitable but these kind of things
might be used in more complex attacks.

Fixes: 832bafa66c9f ("Initial commit of Candlepin module from the original katello-installer.")

Revision a45ac09d - 10/05/2023 01:51 PM - Ewoud Kohl van Wijngaarden

Refs #36760 - Reset candlepin key- and truststore

This takes a 2 step approach where the cached password is removed during
migration (which ends up running during the RPM installation). The
installer then handles replacing the stores when it really runs.

History

#1 - 09/20/2023 09:23 AM - Ewoud Kohl van Wijngaarden

- File 0001-Fixes-36760-Limit-access-to-server.xml.patch added

#2 - 09/28/2023 03:11 PM - Ewoud Kohl van Wijngaarden

- Target version set to 3.8.0

#3 - 10/03/2023 02:46 PM - Ewoud Kohl van Wijngaarden

- File 0001-Refs-36760-Reset-candlepin-key-and-truststore.patch added

This is the installer patch that forces the credentials to also be reset. I started on a proper fix (https://github.com/theforeman/puppet-certs/pull/428), but in the interest of time I'm taking this approach now.

#4 - 10/03/2023 03:13 PM - Eric Helms

And to be clear, you still need root access to do anythng with the password?

#5 - 10/03/2023 03:37 PM - Ewoud Kohl van Wijngaarden

- File deleted (0001-Refs-36760-Reset-candlepin-key-and-truststore.patch)

#6 - 10/03/2023 03:38 PM - Ewoud Kohl van Wijngaarden

- File 0001-Refs-36760-Reset-candlepin-key-and-truststore.patch added

Yes. You can verify this:

```
# ls -l /etc/candlepin/certs/{key,trust}store
-rw-r-----. 1 root tomcat 4687 Oct  3 15:34 /etc/candlepin/certs/keystore
-rw-r-----. 1 root tomcat 4194 Oct  3 15:34 /etc/candlepin/certs/truststore
```

I also had a mistake in the previous patch. I've now verified it on a nightly box.

#7 - 10/04/2023 06:05 PM - Ewoud Kohl van Wijngaarden

- Subject changed from World readable tomcat server.xml contains passwords to CVE-2023-4886: World readable tomcat server.xml contains passwords

- Private changed from Yes to No

Embargo has lifted, removing private.

#8 - 10/04/2023 06:06 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Ewoud Kohl van Wijngaarden

- Pull request https://github.com/theforeman/puppet-candlepin/pull/242 added

#9 - 10/04/2023 06:09 PM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman-installer/pull/886 added

#10 - 10/04/2023 06:11 PM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman-installer/pull/887 added

#11 - 10/05/2023 01:47 PM - The Foreman Bot

- Fixed in Releases 3.9.0 added

#12 - 10/05/2023 02:00 PM - Ewoud Kohl van Wijngaarden

- Status changed from Ready For Testing to Closed

Applied in changeset puppet-candlepin|0f0595d7cbcd1658c09aca173e291ad82217673c.

#13 - 10/05/2023 03:57 PM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman-installer/pull/890 added

#14 - 10/06/2023 11:21 AM - Ewoud Kohl van Wijngaarden

- Fixed in Releases 3.8.0 added

- Fixed in Releases deleted (3.9.0)

Files

0001-Fixes-36760-Limit-access-to-server.xml.patch	1.13 KB	09/20/2023	Ewoud Kohl van Wijngaarden
0001-Refs-36760-Reset-candlepin-key-and-truststore.patch	2.24 KB	10/03/2023	Ewoud Kohl van Wijngaarden