Foreman - Bug #11471

CVE-2015-5246 - previous password still allowed to log into foreman with Active Directory backend

08/24/2015 02:45 PM - larry campbell

Status:	Rejected		
Priority:	Urgent		
Assignee:			
Category:	Authentication		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.9.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/theforeman.org/pull/432		

Description

This was found on Foreman 1.9.0:

I came across this issue by chance. I was forced to change my Active Directory password today. After doing so, I then (mistakenly) attempted to log onto Foreman with my previous password and was able to successfully log in. The new password also worked. I tried with other browsers and even another workstation that I had never logged onto and all attempts allowed me to log on with my non-valid previous password. Perhaps something on foreman/passenger/ruby/etc is caching my credential and not re-checking?

Initial Setup:
Have an Active Directory enviornment available for LDAP Authentication. Setup LDAP Authentication Source in Foreman and have a test user account created in Active Directory.

Steps to recreate:
1. Log on to Foreman with the Active Directory user. This should succeed. Log off.
2. Change your Active Directory account's password.
3. Log on to Foreman with the Active Directory user, and use the previous password. This should fail with authentication denied method, however it succeeds.

History

#1 - 08/31/2015 11:34 PM - Kurt Seifried

Please use CVE-2015-5246 for this issue.

#2 - 09/01/2015 02:56 AM - Dominic Cleal

- Subject changed from previous password still allowed to log into foreman with Active Directory backend to CVE-2015-5246 - previous password still allowed to log into foreman with Active Directory backend

#3 - 09/04/2015 07:27 AM - Dominic Cleal

- Status changed from New to Need more information

Thanks to Daniel for passing this onto foreman-security and confirming the problem.

Just searching though, and I see lots of similar reports against other applications that suggest it's a function of Active Directory and/or the domain controller itself, e.g.

http://serverfault.com/questions/461139/ntlm-auth-can-login-in-ad-with-both-old-and-new-passwords
https://technet.microsoft.com/en-us/library/cc755473%28v=ws.10%29.aspx
https://support.microsoft.com/en-us/kb/906305

Does the login still work an hour later, as that's the claimed timeout of those links?

#4 - 09/07/2015 08:22 AM - Daniel Lobato Garcia

From my tests, neither the connection to LDAP nor logging in work using the old password after the allowed period in HKLM\System\CurrentControlSet\Control\LSA\OldPasswordAllowedPeriod. (Windows registry). If I set that HKLM\System\CurrentControlSet\Control\LSA\OldPasswordAllowedPeriod to 0, the old password will be disabled right away.

#5 - 09/07/2015 08:35 AM - Dominic Cleal

- Status changed from Need more information to Feedback

Thanks Daniel. I'll tentatively close this for now and add the information to our manual and security page.

#6 - 09/07/2015 08:49 AM - Dominic Cleal

- Pull request https://github.com/theforeman/theforeman.org/pull/432 added

- Pull request deleted ()

#7 - 09/08/2015 08:08 AM - larry campbell

I second the observation that the old password failed when we tried it again several hours later. It would make sense this is an AD "feature" as pointed out by Daniel and Dominic, and I support the current method of making users aware through a Foreman Manual notice. Thanks everybody!

#8 - 09/08/2015 08:13 AM - Dominic Cleal

- Status changed from Feedback to Rejected

Thanks for confirming, and for the report Larry. If you come across across any potential security issue in future, please drop us an e-mail to foreman-security@googlegroups.com in case we need to embargo it first. Cheers.