strongSwan - Feature #3014

Support UTF-8 encoded passwords in EAP-MSCHAPv2

05.04.2019 14:04 - Sebastian Thias

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.8.0		
Resolution:	Fixed		

Description

Hi,

I just set up a strongswan-instance with eap-radius bound to a windows-NPS-radius-server using IKEv2 with EAP-MSChapv2. Everything is working fine, except for users that have non-ascii-characters in their passwords. In this case I stumbled upon a password containing an umlaut and the NPS-Server rejects the authentications-request with a "wrong username or password"-message. When exchanging the umlaut with a plain ASCII-letter, everything works as expected. After some digging I found this:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClooCAC

stating that the NPS encodes in extended ASCII rather than UTF-8. Would there be any possibility to configure the encoding used for communicating with a radius-backend?

Thank you very much in advance!

Best regards,
Sebastian

Associated revisions

Revision 4c0d74bc - 16.04.2019 11:26 - Tobias Brunner

eap-mschapv2: Convert UTF-8-encoded passwords

Instead of assuming passwords are simply ASCII-encoded we now assume they are provided UTF-8-encoded, which is quite likely nowadays. The UTF-8 byte sequences are not validated, however, only valid code points are encoded as UTF-16LE.

Fixes #3014.

History

#1 - 05.04.2019 14:11 - Tobias Brunner

- Category set to interoperability

- Status changed from New to Feedback

You are confusing the RADIUS password (to protect the communication with the RADIUS server) with the user passwords verified via EAP-MSCHAPv2. The latter are actually UTF-16 encoded, which strongSwan as client doesn't do, it just uses the password bytes and adds a zero byte to each. As server via RADIUS, strongSwan is not involved in the password verification, though, so if that scenario fails with clients other than strongSwan, it's either those clients' or the RADIUS server's fault.

#2 - 05.04.2019 14:22 - Sebastian Thias

Ok, sorry for the misunderstanding and thanks for the quick reply.

Actually I tried this with the strongswan-app on android and MacOS as client - the behaviour shows the same problems. We also use this NPS-server as an authentication-backend for our 802.1x-wifi-authentication where the password check works flawlessly, this was why I suspected something between strongswan and the NPS to be the issue.

I'll try to investigate further...

#3 - 05.04.2019 14:24 - Tobias Brunner

> Actually I tried this with the strongswan-app on android and MacOS as client - the behaviour shows the same problems.

That's exactly what I'm saying. strongSwan does not support this as client.

#4 - 05.04.2019 14:39 - Sebastian Thias

OK! So you say that the conversion to UTF-16 will go wrong if a multibyte-character is sent in a password-string, because strongswan just pads each password-byte with a 0x00 ?

Is there any chance to change this behaviour?

#5 - 05.04.2019 14:57 - Tobias Brunner

> So you say that the conversion to UTF-16 will go wrong if a multibyte-character is sent in a password-string, because strongswan just pads each password-byte with a 0x00 ?

The password is never sent, this happens on the client during EAP-MSCHAPv2 (source:src/libcharon/plugins/eap_mschapv2/eap_mschapv2.c#L545).

> Is there any chance to change this behaviour?

Unlikely to happen anytime soon (in non-GUI setups you could use pre-prepared NTLM secrets to avoid this issue).

#6 - 05.04.2019 15:20 - Sebastian Thias

So the task would be to include something like this to convert utf-8 to utf-16?

https://doc.freeradius.org/misc_8c_source.html#l00580

#7 - 11.04.2019 09:35 - Tobias Brunner

- Tracker changed from Issue to Feature

- Subject changed from Possible Encoding-Issue between Microsoft NPS and eap-radius to Support UTF-8 encoded passwords in EAP-MSCHAPv2

- Target version set to 5.8.0

- Affected version deleted (5.6.2)

> So the task would be to include something like this to convert utf-8 to utf-16?

Yes, if we assume the password is provided in UTF-8 encoding (which I guess is reasonable nowadays). I pushed something to that effect to the *3014-eap-mschap-utf8* branch.

#8 - 11.04.2019 15:40 - Sebastian Thias

Thank you !!!

#9 - 16.04.2019 16:03 - Tobias Brunner

- Assignee set to Tobias Brunner

- Resolution set to Fixed

I've uploaded a beta version of our Android app that includes this fix to Google Play. Let me know if this works for you.

#10 - 24.04.2019 11:02 - Sebastian Thias

Yes - authenticating via the app towards a Microsoft-NPS-Server via strongswan-eap-radius now also works with German umlauts! Thanks a lot!

#11 - 24.04.2019 11:36 - Tobias Brunner

- Status changed from Feedback to Closed

> Yes - authenticating via the app towards a Microsoft-NPS-Server via strongswan-eap-radius now also works with German umlauts! Thanks a lot!

Thanks for testing. The app is now live.

#12 - 24.04.2019 11:50 - Sebastian Thias

Wonderful! Thank you very much for your incredibly quick and valuable communication and help!