TLS 1.2 and updated RADIUS requirements

Created - 12/11/2015

Reformatted and updated - 15/12/2021

Original version: Alan Buxey

Original document:
https://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/EWIG3ubfzHJPurR... [1]

TLS 1.2 negotiation in forthcoming OS releases require sites running RADIATOR, FreeRADIUS 2 and FreeRADIUS 3 to upgrade, NPS sites may need reconfiguring.

Overview

At the time of writing (Nov 2015), testing with the then forthcoming OS releases - wpa_supplicant 2.4 (wpa_supplicant is used in Android and Linux) - revealled issues with TLS 1.2 negotiation with various RADIUS servers that were tested against. iOS 9 and OSX El Capitan had shown this issue in beta/pre-release but now do not (Nb. apparently Apple deferred using TLS 1.2 in iOS9 - El Capitan to be confirmed - due to the issue with many RADIUS servers around the world....this issue WILL arise for this platform at some time in the future though). Android 6.0 (Marshmallow) was exhibiting similar behaviour.

RADIATOR

Radiator uses the Net::SSLeay for its SSL support. If you are running older versions, these may come via your OS repository, eg version 1.35, these will not work with TLS 1.2 negotiation if you are running RADIATOR 4.14 or 4.15. Advice - upgrade to Net::SSLeay 1.70 (and whilst looking at this, upgrade to RADIATOR 4.15 *with the recent patchset which fixes MPPE key issue* - many bug fixes and some great new features such as REDIS support)

FreeRADIUS 3

FreeRADIUS3 < 3.0.6 does not DO TLS 1.2 negotiation either. To ensure support with newer clients this feature was added (at same time as 2.2.6) - with similar issue. Upgrade to 3.0.10 (which also has the same x509 security fix from 3.0.9 too) - Sites running OpenSSL 1.0.2 need 3.0.11(!)

(if building FreeRADIUS locally, please ensure that the server you are running FreeRADIUS on has same version of OpenSSL as the server you built the FreeRADIUS on - next releases have a bug-reversion that ensures that this is the case)

Microsoft NPS

With Windows Server 2012, support for TLS 1.2 was introduced via update Security Update for Windows Server 2012 (KB2977292). (Ignore the dated document at https://support.microsoft.com/en-us/kb/2719195 [2] - which is no longer available).

Read the following advisory regarding TLS 1.2 support being added to the OS: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2014/2977292?redirectedfrom=MSDN [3] (was https://technet.microsoft.com/en-us/library/security/2977292.aspx [4]) and https://support.microsoft.com/en-us/kb/2977292 [5]. This states that to enable TLS after you install the security update, you must add a DWORD value that is named TlsVersion to the following registry subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\PPP\EAP\13

The value of this registry key can be 0xC0, 0x300, 0xC00, or any OR'ed combination of these values if you want to support multiple TLS versions. The configuration can be done on both the EAP client and the EAP server.

An update was also made available for Windows Server 2008 at the same time: https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-for-microsoft-eap-implementation-that-enables-the-use-of-tls-october-14-2014-d9ba4b83-b4e9-2c01-83a7-e42706e671af [6] and https://www.dot11.guru/2020/07/27/enforcing-tls-1-2-for-microsoft-nps-server-2008-2012/ [7]

An up to date matrix of TLS version support/enablement is published on Protocols in TLS/SSL (Schannel SSP) https://docs.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp- [8]

With Windows Server 2016 onwards TLS 1.2 is enabled by default https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings [9] (ref. Windows Server 2016, 2019 and 2022)

Organisations still using Windows Server 2012 should enable TLS 1.2 (but since some client devices do not support TLS 1.2, 1.0 and 1.1 should remain enabled). This technet forum article indicate how: https://social.technet.microsoft.com/Forums/en-US/835a7bd5-3b9e-460c-bb5e-a971d05d828f/default-tls-settings-on-windows-server-2016?forum=ws2016 [10]

ISE 2.0

Apparently does TLS 1.2 - certainly now supports EAP-TTLS (http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/release_notes/ise2... [11])

Older RADIUS platforms

FreeRADIUS 2 < 2.2.6 should not have an issue as it doesnt DO TLS 1.2 negotiation. This may have *other* adverse effects with clients that try doing TLS 1.2 (we dont know, for example, what forthcoming Windows Phone releases will do) - however, 2.2.6 and 2.2.7 DO have issues - upgrade to 2.2.9 (which also has an x509 security issue fix from 2.2.8 anyway). Sites running OpenSSL 1.0.2 need 2.2.10(!)

FreeRADIUS 1.x or 2.1.x , Microsoft IAS, ACS 3.x or 4.x and ISE 1.0 or 1.1 are not supported

or reviewed.

ACS 5 - untested/unknown

ISE 1.2/1.3 - untested/unknown

obnote: You might also want to check out my blog about the requirements for larger DH keys on your RADIUS server:

https://community.jisc.ac.uk/blogs/8021x-clients-and-radius-server-suppo... [12]

obnote2: on RADIATOR/FreeRADIUS platforms, ensure your OpenSSL package is the latest possible copy - keep your OS up to date.

Source URL: https://community.jisc.ac.uk/library/network-and-technology-service-docs/tls-12-and-updated-radius-requirements

Links
[1] https://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/EWIG3ubfzHJPurR4zFGpMlIBf2Vhi0y0nvyvIdbsYWTTMg
[2] https://support.microsoft.com/en-us/kb/2719195
[3] https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2014/2977292?redirectedfrom=MSDN
[4] https://technet.microsoft.com/en-us/library/security/2977292.aspx
[5] https://support.microsoft.com/en-us/kb/2977292
[6] https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-for-microsoft-eap-implementation-that-enables-the-use-of-tls-october-14-2014-d9ba4b83-b4e9-2c01-83a7-e42706e671af
[7] https://www.dot11.guru/2020/07/27/enforcing-tls-1-2-for-microsoft-nps-server-2008-2012/
[8] https://docs.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-
[9] https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings
[10] https://social.technet.microsoft.com/Forums/en-US/835a7bd5-3b9e-460c-bb5e-a971d05d828f/default-tls-settings-on-windows-server-2016?forum=ws2016
[11] http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/release_notes/ise20_rn.html#pgfId-591302
[12] https://community.jisc.ac.uk/blogs/8021x-clients-and-radius-server-supporting-bigger-diffie-hellman-dh-keys