TLS 1.0 and TLS 1.1 soon to be disabled in Windows

By Jessica Krynitsky

Published Aug 01 2023 11:28 AM 213K Views

Learn about the upcoming changes in Schannel protocol defaults and how to remove dependencies on legacy TLS versions or keep them enabled for compatibility.

Overview

Transport Layer Security (TLS) is the most common internet protocol for setting up an encrypted channel of communication between a client and server. TLS 1.0 dates back to 1999 and, over time, several security weaknesses have been found in this protocol version. TLS 1.1 was published in 2006 and made some security improvements, but never saw broad adoption. These versions have long been surpassed by TLS 1.2 and TLS 1.3, and TLS implementations try to negotiate connections using the highest protocol version available.

Over the past several years, internet standards and regulatory bodies have deprecated or disallowed TLS versions 1.0 and 1.1, due to a variety of security issues. We have been tracking TLS protocol usage for several years and believe TLS 1.0 and TLS 1.1 usage data are low enough to act.

To increase the security posture of Windows customers and encourage modern protocol adoption, TLS versions 1.0 and 1.1 will soon be disabled by default in the operating system, starting with Windows 11 Insider Preview builds in September 2023 and future Windows OS releases. This change applies to both client and server, but it will not impact any in-market OS versions. There is an option to re-enable TLS 1.0 or TLS 1.1 for users who need to maintain compatibility.

Diagnostic events

Applications that start failing when TLS 1.0 and TLS 1.1 are disabled can be identified by Event 36871 in the Windows Event Log.

Sample Event:

A fatal error occurred while creating a TLS <client/server> credential. The internal error state is 10013. The SSPI client process is <process ID>.

Co-Authors

jess_krynitsky

Andrej_Popov

Version history

Last update: Aug 10 2023 04:15 PM

Updated by: jess_krynitsky

Labels

Device management	88
Security	84
Windows 10	98
Windows 11	173

Share

The impact of this change depends largely on the Windows applications using TLS. For example, TLS 1.0 and TLS 1.1 have already been disabled by Microsoft 365 products as well as WinHTTP and WinINet API surfaces. Most newer versions of applications support TLS 1.2 or higher protocol versions. Therefore, if an application starts failing after this change, the first step is to look for a newer version of the application that has TLS 1.2 or TLS 1.3 support.

It's recommended to use the system default settings for the best balance of security and performance. If organizations limit TLS cipher suites using Group Policy or PowerShell cmdlets, they should also verify that cipher suites needed for TLS 1.3 and TLS 1.2 are enabled.

If there are no alternatives available and TLS 1.0 or TLS 1.1 is needed, the protocol versions can be re-enabled with a system registry setting. To override a system default and set a (D)TLS or SSL protocol version to the Enabled state, create a DWORD registry value named "Enabled" with an entry value of "1" under the corresponding version-specific subkey. Examples of TLS 1.0 subkeys are as follows:

HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client

HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server

> **Note:** Re-enabling TLS 1.0 or TLS 1.1 on machines should only be done as a last resort, and as a temporary solution until incompatible applications can be updated or replaced. Support for these legacy TLS versions may be removed completely in the future.

Guidance for SSPI application developers

Although most applications and services use Schannel via HTTP and .NET APIs, some call the Security Support Provider Interface (SSPI) directly. Historically, SSPI callers implementing TLS clients and servers would pass the SCHANNEL_CRED structure when calling AcquireCredentialsHandle(). This allowed the hard coding of legacy TLS versions and prevented apps from using new TLS versions. With TLS 1.0 and TLS 1.1 disabled by default, an SSPI application that only allows these versions will fail to connect.

SCHANNEL_CRED was deprecated in Windows 10, and SSPI callers should specify their preferences using SCH_CREDENTIALS instead. Applications using this new structure will be able to negotiate TLS 1.3 and later protocol versions. When updating code to switch from SCHANNEL_CRED to SCH_CREDENTIALS, implementers should test their TLS client or server against a TLS 1.3 peer and ensure that the code correctly handles SEC_I_RENEGOTIATE returned from DecryptMessage().

For more information on finding and removing application dependencies on TLS 1.0 and 1.1, please refer to Solving the TLS 1.0 Problem.

Known issues

We have tested this change against top Windows applications, and found that the following versions rely on TLS 1.0 or TLS 1.1 and are expected to be broken.

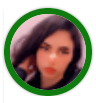
> **Note:** This is not an exhaustive list. All systems and organizations should test the disablement using the steps described above and observe any failures. Please reach out directly to the application owner, as they often have an updated version or mitigation available.

- SQL Server - 2012, 2014, 2016 (see KB3135244 - TLS 1.2 support for Microsoft SQL Server - Microsoft Support for how to upgrade to TLS 1.2 support)
- Microsoft Office 2008 Professional - Accounting Express
- Xbox One SmartGlass - 2.2.1702.2004
- Project Plan 365 - 23.8.1204.14137
- Safari - 5.1.7
- EVault Data Protection - 7.01.6125
- Turbo Tax - 2017, 2014, 2011, 2012, 2016, 2015, 2018
- BlueStacks 3 (蓝叠3) - 5.10.0.6513
- BlueStacks X - 0.21.0.1063
- Splice - 4.0.35686, 4.2.4
- Driver Support - 10.1.2.41, 10.1.4.20
- K7 Enterprise Security and 4.1.0.116
- DRUKI Gofin - 3.17.63.0
- vWorkspace - 8.6.1
- ARMA 3
- LANGuard - 12.7.2022.0406
- Adguard - 6.4.1814.4903, 7.12.41.70.0
- 火萤视频桌面 - 5.2.5.9
- CCB Security Client (中国建设银行E路航网银安全组件) - 3.3.8.4
- ArcGIS - 10.3.3400
- ACDSee Photo Studio – 2018, 2023
- Blio e-Reader - 3.4.0.9728, 3.4.1.9759

Continue the conversation. Find best practices. Bookmark the Windows Tech Community and follow us @MSWindowsITPro on Twitter. Looking for support? Visit Windows on Microsoft Q&A.

15 Likes

29 Comments



HotCakeX MVP

Aug 01 2023 11:56 AM

Great change!

1 Like

Hadzhigeorgiev Brass Contributor

Aug 02 2023 06:55 AM

It was a long wait

1 Like

chasapple4 Copper Contributor

Aug 03 2023 02:44 PM

This will semi brick many HP printers as HP has failed to enabled TLS 1.2 on many HP printers (you can't access the printers embed web server for most settings if you have TLS 1.2+ only)

2 Likes

LuigiBruno Steel Contributor

Aug 09 2023 01:39 AM

Noted.
I've been working on this hardening for several months, this will save time.

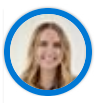
1 Like

Brian Roehm Copper Contributor

Aug 15 2023 08:18 AM

We tested TLS1.2 only setups a while back and found the Onprem Dynamics GP still seems to use TLS 1.0. Clients could not connect to the server. How do you go about tracking down and fixing whatever pieces of a program like GP (with so many things going on) are using the (very) soon to be deprecated protocol?

1 Like

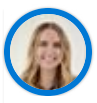


jess_krynitsky Microsoft

Aug 17 2023 09:51 AM

@chasapple4 thank you for the heads-up about HP printers relying on TLS 1.0/1.1, we will be sure to engage with them. I believe we have the right mitigations in place to prevent this being an issue. As of now, there are no plans to bring this change to any in-market Windows OS via update. The hope would be that the newest printers on future OS versions will support TLS 1.2+. Additionally, the registry keys or group policy can re-enable the legacy protocols if necessary for backwards compatibility, and we can work directly with HP to ensure they have the tools to support their customers and prevent any bricked devices.

1 Like



jess_krynitsky Microsoft

Aug 17 2023 10:05 AM

@Brian Roehm thank you for your question:
> How do you go about tracking down and fixing whatever pieces of a program like [Onprem Dynamics] GP (with so many things going on) are using the (very) soon to be deprecated protocol?

First, I should note that the known issues list in this blog is only a subset of Windows applications that rely on TLS 1.0/1.1. We have an outreach program that has already engaged with the developers of every application listed here, and more, and many

mitigation. We will soon post known issues in a more permanent MSLearn document page where we can update the list with additions, fixes, and resolutions.

We are taking a data-driven approach to this deprecation and will continue to engage with applications which pose a significant risk to customers. That being said, we cannot possibly engage with every single application developer in the ecosystem. We hope that spreading awareness with announcements like this one along with the upcoming Insider Preview release will spur both organizations and applications to make the switch. We strongly encourage customers to engage directly with application owners to ensure they are aware this change is coming and put the onus on them to provide a solution or workaround.

1 Like

chasapple4 Copper Contributor

Aug 17 2023 02:22 PM

@jess_krynitsky It is a bunch of home inkjet printers from HP and HP has refused to enable TLS 1.2 on them even tho they are less than 8 years (the only way to manage any advanced features is via HP Smart app (many browsers have already dropped support for TLS 1.1 and lower)

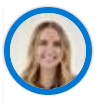
1 Like

Alearnhabit Copper Contributor

Sep 21 2023 09:17 AM

Has anyone seen issues with RDP stop functioning after disabling TLS1.0 and 1.1, along with older ciphers?

0 Likes

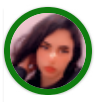


jess_krynitsky Microsoft

Sep 22 2023 09:50 AM

@Alearnhabit Which Windows version were you using when you observed the RDP and cipher failures?

0 Likes



HotCakeX MVP

Sep 23 2023 09:27 AM

@Alearnhabit No, never.

0 Likes

Ed_Bishop Copper Contributor

Oct 11 2023 02:55 PM

Is there any kind of ETA as to when this is going to get rolled out?

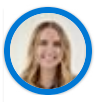
0 Likes

yoursearchdude Copper Contributor

Oct 18 2023 08:14 AM

still no update from MS. @jess_krynitsky is it already out with preview build for testing?

0 Likes



jess_krynitsky Microsoft

Oct 18 2023 12:31 PM

We are actively working to resolve application compatibility issues to mitigate user impact before releasing the default disablement to Windows Insider Preview. Please watch this space for updates. You can also look for upcoming Insider release notes for preview builds with TLS 1.0/1.1 disabled.

1 Like

GerardoHernandez Brass Contributor

Jan 30 2024 02:10 PM

Hi @jess_krynitsky

Is there any timeline on when this will be deployed to production?

Regards,

0 Likes

J-C-L Copper Contributor

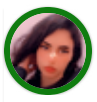
Feb 05 2024 06:22 AM

about time,

Will this also disable old SSL versions too?

Also, when will this update be pushed out?

0 Likes



HotCakeX MVP

Mar 04 2024 01:21 PM

@J-C-L It's most likely coming out in Windows 11 24H2 update. Older SSL versions won't work. They already don't work for many systems, Edge for example only uses TLS 1.2 and 1.3 and PowerShell doesn't use older ones.

0 Likes

chasapple4 Copper Contributor

Mar 04 2024 05:57 PM

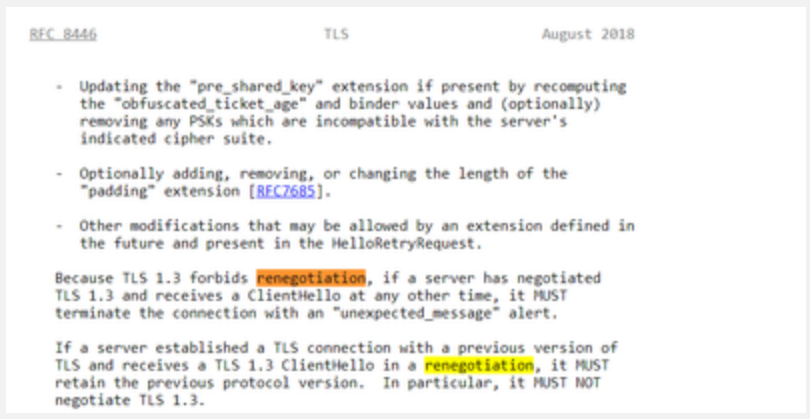
@J-C-L SSL pre TLS 1.0 has been disabled in most browsers for

0 Likes

JohnT0859 Copper Contributor

Mar 25 2024 06:16 PM

I've been testing Schannel with TLS1.3 and am handling the renegotiate on (the first) Decryptmessage.
Question though the RFC for TLS1.3 explicitly forbids renegotiation.
Is there something I'm missing ?



RFC 8446 TLS August 2018

- Updating the "pre_shared_key" extension if present by recomputing the "obfuscated_ticket_age" and binder values and (optionally) removing any PSKs which are incompatible with the server's indicated cipher suite.
- Optionally adding, removing, or changing the length of the "padding" extension [RFC7685].
- Other modifications that may be allowed by an extension defined in the future and present in the HelloRetryRequest.

Because TLS 1.3 forbids renegotiation, if a server has negotiated TLS 1.3 and receives a ClientHello at any other time, it MUST terminate the connection with an "unexpected_message" alert.

If a server established a TLS connection with a previous version of TLS and receives a TLS 1.3 ClientHello in a renegotiation, it MUST retain the previous protocol version. In particular, it MUST NOT negotiate TLS 1.3.

0 Likes

Warner777 Copper Contributor

Jun 12 2024 05:29 AM

Windows Server 2016 Nuget.exe default version uses TLS 1.0 and so to upgrade Nuget you will need to enable TLS 1.0 upgrade Nuget and then re-disable TLS 1.0.

0 Likes

jess_krynitsky Microsoft

Jun 17 2024 12:30 PM

@Warner777 This change in defaults will only apply to new Windows desktop and Server SKUs, so it will not affect Windows Server 2016 (nor 2019 or 2022). That being said, if you were to manually disable TLS 1.0/1.1, then yes that would apply.

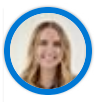
1 Like

jess_krynitsky Microsoft

Jun 17 2024 02:08 PM

@JohnT0859
SEC_I_RENEGOTIATE is not (only) an indication of renegotiation. Its original use was renegotiation, but we cannot add new return values for compatibility reasons. So it is used for everything post-handshake in TLS 1.3.
It means a post-handshake message has been received and the SSPI caller needs to return to the handshake loop.
This is all described in DecryptMessage (Schannel) function - Win32 apps | Microsoft Learn

1 Like



jess_krynitsky Microsoft

Jun 17 2024 02:11 PM

There is understandably some confusion around the release time for this change to Windows default TLS protocols. Please note that we are gradually testing this change with the **Windows Insider Preview** program, and **bringing the new defaults to official Windows versions has been delayed** due to a large number of incompatible 3rd party applications.

1 Like

jkazbill Copper Contributor

Jul 12 2024 10:11 AM

I disabled TLS 1.0 and 1.1 on a server via GPO. I've confirmed that the settings in the registry are correct and working. I attempted to connect to the server using openssl and I got an error on my client as I would expect, but an event with ID 36871 did not appear in the Windows System event log. Event logging is enabled in the registry key HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL. The value is EventLogging - REG_DWORD - 0x00000001 (1).

Also, I've only disabled TLS 1.1 for incoming (Server) connections. Outbound (Client) connections are still allowed to use TLS 1.1. TLS 1.0 is disabled for both inbound and outbound connections.

Have you seen this before and do you have any recommedations?

0 Likes

jess_krynitsky Microsoft

Jul 12 2024 10:57 AM

@jkazbill It is possible that the event is being logged as a warning or informational event, and the default event logging reg key value of 1 only logs error messages. Event ID 36871 is an error message, but perhaps it logged a different event. If you would like to troubleshoot, I would recommend increasing the event logging level following this guidance: Enable Schannel event logging in Windows - Internet Information Services | Microsoft Learn and looking for other Schannel events, described here: Schannel Events | Microsoft Learn. Thank you for your feedback!

0 Likes

jkazbill Copper Contributor

Jul 12 2024 12:02 PM

@jess_krynitsky, thank you for the information!

I want to get some clarification on "Applications that start failing when TLS 1.0 and TLS 1.1 are disabled can be identified by Event 36871 in the Windows Event Log."

I originally interpreted that as meaning that 36871 is logged when a remote machine attempts to connect to the server using TLS 1.0 or 1.1. Does it mean, instead, that when an application starts up on the server and it attempts to create a TLS 1.0 or 1.1 credential then 36871 is logged?

I was hoping to use 36871 to identify failed inbound connections after I disable TLS 1.1. That why I can more quickly re-enable TLS 1.1 and then address those systems attempting to connect using TLS 1.1 to ensure they start using a stronger protocol.

0 Likes

jkazbill Copper Contributor

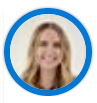
Jul 12 2024 12:33 PM

@jess_krynitsky, I looked up the description of 36871 at Schannel Events | Microsoft and it looks like it is specific to SMTP. Is there another event ID that we should look for from a diagnostic standpoint?

Event ID 36871: A Fatal Error Occurred While Creating An SSL (client or server) Credential
This behavior is caused by the SMTP service processing an incoming EHLO command if no certificate is assigned to an SMTP site. This message is logged twice, once when the SMTP service starts, and once when the first EHLO command is received.

Simple Mail Transfer Protocol (SMTP) controls how email is transported and then delivered across the Internet to the destination server. The SMTP EHLO command enables the server to identify its support for Extended Simple Mail Transfer Protocol (ESMTP) commands.

0 Likes



jess_krynitsky Microsoft

Jul 12 2024 04:43 PM

@jkazbill

> I originally interpreted that as meaning that 36871 is logged when a remote machine attempts to connect to the server using TLS 1.0 or 1.1. Does it mean, instead, that when an application starts up on the server and it attempts to create a TLS 1.0 or 1.1 credential then 36871

This is correct, failure to create a credential is logged on the machine where the credential is being created, client or server. Unfortunately the doc description specific to SMTP is outdated, Event 36871 is generic to SSPI. The internal error state 10013 in the sample event indicates that the failure to create a credential is due to a mismatch of application-specified protocols and enabled system protocol versions, such as TLS 1.0 or TLS 1.1.

For remote client connections failing due to TLS version mismatch with the server, there is a different warning event generated (e.g., Event 36874). It is not very helpful for analysis, other than statistical measurement of failures, because we don't know where the connection came from (no networking details) or if it was specific to TLS 1.0/1.1 or a mismatch of cipher suites.

If HTTP.SYS/IIS is used on the server, HTTP.SYS logs will identify the IP address of the failing remote peer. This may be a better option for your use case.

I hope this helps! And thank you for the feedback, I will take a note to clarify the event log details in our permanent MSLearn page for this content, as well as ensure the Schannel Event log descriptions are up-to-date.

1 Like

DeepakM2130 Copper Contributor

Oct 29 2024 05:50 PM

When the change will be implemented? We still see the TLS 1.0 and 1.1 in Windows 11 24H2.

0 Likes

You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in.

Comment