# What's in that patch? May 2017

Updated 5/9/2017

## Table of Contents

## Download Links

- http://www.toddklindt.com/sp2013builds
- http://www.toddklindt.com/sp2016builds
- https://sharepointupdates.com/Patches

## Fix Count

| KB | |
|---|---|
| Security update for SharePoint Foundation 2013: May 9, 2017 (KB3191914) | 1 |
| May 9, 2017, update for SharePoint Server 2013 (KB3191825) | 4 |
| Security update for SharePoint Server 2013: May 9, 2017 (KB3191886) | 9 |
| Security update for SharePoint Server 2013: May 9, 2017 (KB3178633, KB3172532, KB3172536, KB3162068, KB3172475) | 5 |
| Security update for Project Server 2013: May 9, 2017 (KB3191890) | 3 |
| Security update for SharePoint Server 2013: May 9, 2017 (KB3162069) | 1 |
| Security update for SharePoint Foundation 2013: May 9, 2017 (KB3162054) | 1 |
| Security update for SharePoint Server 2013: May 9, 2017 (KB3178638) | 1 |
| Security update for SharePoint Server 2013: May 9, 2017 (KB3172482) | 1 |
| Security update for Word Automation Services on SharePoint Server 2013: May 9, 2017 (KB3162040) | 1 |
| Security update for Excel Services on SharePoint Server 2013: May 9, 2017 (KB3191887) | 1 |
| | **28** |
| May 9, 2017, update for SharePoint Server 2016 (KB3191884) | 2 |
| May 9, 2017, Description of the security update for SharePoint Server 2016 (KB3191880) | 9 |
| | **11** |

## Description of the security update for SharePoint Foundation 2013: May 9, 2017 (KB3191914)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0255.

## May 9, 2017, update for SharePoint Server 2013 (KB3191825)

This update contains the following improvements and fixes:

- When you use a screen reader, it's difficult to determine which attachment that you are deleting, because the delete link isn't conceptually linked to the related attachment. Meanwhile, if you tab through the page, you may find that the delete link of the attachment is out of order.
- Enables you to create site collections in SharePoint Online in a hybrid environment (the Hybrid Admin Site Collection Creation - Default to Cloud feature).
- Improves the strings for the Hybrid Extranet Site Creation Default to Cloud feature.
- Translates some terms in multiple languages to make sure that the meaning is accurate.

## Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3191886)

This security update contains the following improvements:

- Updates flags for the ParentLink managed property to match the DocumentLink managed property.
- Improves execution efficiency of the stored procedure for deleting Secure Store audits.
- Improves word breaking for Thai language.

This security update fixes the following nonsecurity issues:

- You can't restore a document of a document set to an earlier version if the document library contains more than 5,000 items.

- After you delete an organization unit for an AD Import connection, the deleted organization unit is still shown as selected.
- Notification emails that indicate that a page will expire contain an invalid link.
- You can't create more than 200 content deployment jobs in SharePoint Server 2013.
- A screen reader reads out the term icons in a term hierarchy tree view.
- After you delete a search center sub site, you can't download search reports any more.

### Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3178633)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

### Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3172532)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

### Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3172536)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

### Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3162068)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3172475)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for Project Server 2013: May 9, 2017 (KB3191890)

This security update fixes the following nonsecurity issues:

- Some summary resource assignment work or actual work values may have large negative numbers. This issue may cause the project publish process to fail.
- When you create a project web app instance at the root, and then you create project sites under a different site collection, you can't use the project details link in the project sites to return to the project. Instead, you may see an error message that resembles the following:

  This page can't be displayed

  Make sure the web address http://projectdrilldown.aspx is correct.

  Look for the page with your search engine.

  Refresh the page in a few minutes.
- Consider the following scenario:

  In project professional, you publish a project that contains a collapsed summary task.

  You open the project in Project Web App, and then you edit the project.

  You apply a filter to the project that sets criteria that should display tasks that are underneath the collapsed summary task.

  In this scenario, tasks that should appear do not appear.

## Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3162069)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for SharePoint Foundation 2013: May 9, 2017 (KB3162054)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3178638)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for SharePoint Server 2013: May 9, 2017 (KB3172482)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for Word Automation Services on SharePoint Server 2013: May 9, 2017 (KB3162040)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0254 and Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## Description of the security update for Excel Services on SharePoint Server 2013: May 9, 2017 (KB3191887)

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0281.

## May 9, 2017, update for SharePoint Server 2016 (KB3191884)

This update includes the following improvements and fixes:

- After you apply an update for a SharePoint language pack, certain performance counters are deleted but are not recreated. This causes the ULS logs to flood with error messages because of the missing performance counters. After you install this update, performance counters are no longer deleted in this case. The previously deleted performance counters will be recreated.

- Translates some terms in multiple languages to make sure that the meaning is accurate.

## May 9, 2017, Description of the security update for SharePoint Server 2016 (KB3191880)

This security update contains the following improvements:

- Enable administrators to change document parsing timeout and memory limit.

- Adds a **PreserveDeletedUserMetadataReferences** switch to Import-SPWeb. Adding this switch lets references to deleted users who are referenced by the list item author and editor metadata be preserved.

- Translates some terms in multiple languages to make sure that the meaning is accurate.

This security update fixes the following nonsecurity issues for Project Server 2016:

- The March 2017 public update provided the necessary WSDL files in order to programmatically access the Project Server Interface (PSI). However, the WDSL files were not completely correct. Therefore, even after the update is installed, it wasn't possible to access the various PSI end points.

- When you run an administrative backup and an administrative restore of Enterprise custom fields, the restore fails at 29 percent completion. You also see a DatabaseForeignKeyViolationError (50002) queue error.

This security update fixes the following nonsecurity issues for SharePoint Server 2016:

- When you lose SharePoint sites that are upgraded from SharePoint 2013 to SharePoint 2016, sites fail to load because of multiple web parts not upgrading and referencing the

wrong version. SSRS Web Part and SPListFilter are two examples. After you install this update, the upgrade of such pages will complete without errors.

- When you run an administrative backup and an administrative restore of Enterprise custom fields, the restore fails at 29 percent completion. You also see a DatabaseForeignKeyViolationError (50002) queue error.

- For remote SharePoint calls in hybrid, the query rewrite in the result source is added to the query two times. This could cause an unexpected recall for custom query rewrites.

- SharePoint outbound email messages incorrectly try to authenticate to SMTP servers that support Generic Security Service Application Program Interface (GSSAPI), Kerberos, or NTLM authentication. This may prevent email messages from being sent. After you install this update, SharePoint sends email messages anonymously without authentication.