# What’s in that patch? October 2019

Updated 10/14/2019

## Table of Contents

## Download Links

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

## Fix Count

| | |
|---|---:|
| **SharePoint 2013** | **3** |
| Description of the security update for SharePoint Enterprise Server 2013: October 8, 2019 | 1 |
| Description of the security update for SharePoint Foundation 2013: October 8, 2019 | 1 |
| Description of the security update for SharePoint Enterprise Server 2013: October 8, 2019 | 1 |
| | |
| **SharePoint 2016** | **10** |
| October 8, 2019, update for SharePoint Enterprise Server 2016 (KB4484115) | 1 |
| Description of the security update for SharePoint Enterprise Server 2016: October 8, 2019 | 9 |
| | |
| **SharePoint 2019** | **11** |
| October 8, 2019, update for SharePoint Server 2019 Language Pack (KB4484109) | 2 |
| escription of the security update for SharePoint Server 2019: October 8, 2019 | 9 |

## Description of the security update for SharePoint Enterprise Server 2013: October 8, 2019

This security update contains a fix for the following nonsecurity issue:

- If you visit a Content Search Web Part (CSWP) from the Google page viewer, or if you set the **AlwaysRenderOnServer** boolean value in a CSWP to **True**, the web part displays no content after update 4461549 is applied. After the update is applied, the CSWP works as expected.

## Description of the security update for SharePoint Foundation 2013: October 8, 2019

This security update contains a fix for the following nonsecurity issue:

- If you visit a Content Search Web Part (CSWP) from the Google page viewer, or if you set the **AlwaysRenderOnServer** boolean value in a CSWP to **True**, the web part displays no content after update 4461549 is applied. After this update is applied, CSWP works as expected.

## Description of the security update for SharePoint Enterprise Server 2013: October 8, 2019

- This security update resolves a remote code execution vulnerability that exists in Microsoft Excel software when the software fails to correctly handle objects in memory. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2019-1331.

## Description of the security update for SharePoint Enterprise Server 2016: October 8, 2019

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

- Fixes a problem with the **Convert-SPWebApplication** cmdlet when the User Principal Name (UPN) is set as an identifier. Now you will be able to move SharePoint authentication to the Active Directory Federation Services (AD FS) Identity Provider by using following command:

  ```
  Convert-SPWebApplication -Identity $wa -From CLAIMS-WINDOWS -To
  CLAIMS-TRUSTED-DEFAULT -TrustedProvider $tp
  ```

- Fixes the issue that affects access to the host-named site collection if one of the sites is deleted and users lose access to other sites for about a day. Now users will be able to access all the sites by running following command in PowerShell even though one of the sites is deleted:

```
$config = Get-SPSecurityTokenServiceConfig

$config.WindowsModeIgnoreCache = $true

$config.Update()
```

- Users who have limited permissions on a list or document library but have approve-level permissions on a folder can now approve multiple items or documents in the folder. To complete the approval, you must select the items in the folder and use the **Approve/Reject** option on the Ribbon.
- SharePoint patching may copy more folders than are necessary for side-by-side patching. This consumes additional hard drive space. This update fixes the issue by restricting copying to only the folders that are necessary for side-by-side patching.

This security update contains improvements and fixes for the following nonsecurity issues in Project Server 2016:

- Makes changes to display the new Japanese era name for date format samples in **Date Format** in Project Web App (PWA) sites.
- The **OwnerId** property is now available to update the project owner through a REST call. The type of this property is **String**, but it accepts only the user's numeric ID.
- You cannot delete resource calendar exceptions through the client-side object model (CSOM). This issue occurs after you install update 4464594.
- If the stage status information text contains special characters such as an ampersand (&), workflows fail.
- When the Schedule Variance Percentage (SVP) or Cost Variance Percentage (CVP) earned value becomes very large, this creates an overflow condition. This causes the client-side object model (CSOM) or REST calls that are made while accessing the project to fail. The SVP and CVP values now have a lower limit of "-100%" and upper limit of "100%."

## Description of the security update for SharePoint Enterprise Server 2016: October 8, 2019

- In this update, PerformancePoint Dashboard Designer now uses SHA256 digital signatures to verify the authenticity of files.

## October 8, 2019, update for SharePoint Server 2019 Language Pack (KB4484109)

This update contains the following improvement and fix:

- With this update, PerformancePoint Dashboard Designer now uses SHA256 digital signatures to verify the authenticity of files.
- When you select **View Installed Updates** in the Windows Control Panel, you see the most recently installed SharePoint Server 2019 Public Updates listed. However, the version number of these updates isn't displayed in the **Version** column. After you install this update, the version number of these updates will be displayed.

## Description of the security update for SharePoint Server 2019: October 8, 2019

This security update contains improvements and fixes for the following nonsecurity issues:

- A crawl of content that has many links fails because the number of links exceeds the maximum allowable. After multiple failures, the search index entries for the content are deleted unexpectedly. After this update is applied, you can set the maximum number of links to be sent to the index by using the **ContentPIMaxNumLinks** property.

  For example, you can run the following PowerShell commands in the SharePoint 2019 Management Shell to set **ContentPIMaxNumLinks** to **10000**:

  ```
  $ssa = Get-SPEnterpriseSearchServiceApplication

  $ssa.SetProperty("ContentPIMaxNumLinks", 10000)

  $ssa.Update()
  ```

- When you select **View Installed Updates** in the Windows Control Panel, you see the most recently installed SharePoint Server 2019 Public Updates listed. However, the version number of these updates isn't displayed in the **Version** column. After you install this update, the version number of these updates is displayed.
- Search and Distributed Cache servers in a MinRole farm that have custom web templates display "Upgrade Required" after you run an in-place build-to-build upgrade. After this update is applied, the servers display "No Action Required."
- When you access a classic Team site and open the browser's developer console, you see an error message that states "CSS3111: @font-face encountered unknown error. Office365Icons.eot." After you install this update, there is no error.
- Fixes an issue in which the stage status information text contains special characters such as an ampersand (&), workflows fail.

- Makes changes to display the new Japanese era name for date format samples in **Date Format** in Project Web App (PWA) sites.
- You can now update a task dependency lead and lag time by using the **LinkLagDuration** property through the client-side object model (CSOM). Similar to other duration properties (such as the **Task.Duration** property in the Task Object), it excepts either a string or an integer value. For example, either **1d** or **480** is acceptable to indicate one day of work.
- The **CalendarException.RecurrenceWeek** property returns wrong values for calendar exceptions through the client-side object model (CSOM).
- When the Schedule Variance Percentage (SVP) earned value becomes very large, an overflow condition occurs. This may cause either abnormal SVP values within Project Web App (PWA) project views or the view may fail to load. The SVP value now has a lower limit of "-100%" and upper limit of "100%".