What's in that patch? November 2019

Updated 12/15/2019

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: November 12, 2019	1
November 12, 2019, cumulative update for SharePoint Enterprise Server 2013 (KB4484155)	2
SharePoint 2016	**9**
Description of the security update for SharePoint Enterprise Server 2016: November 12, 2019	8
November 12, 2019, update for SharePoint Enterprise Server 2016 (KB4484147)	1
SharePoint 2019	**13**
Description of the security update for SharePoint Server 2019: November 12, 2019	11
Description of the security update for SharePoint Server 2019 Language Pack: November 12, 2019	2

Description of the security update for SharePoint Enterprise Server 2013: November 12, 2019

This security update resolves an information disclosure vulnerability that exists if Microsoft Excel incorrectly discloses the contents of its memory. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2019-1446.

November 12, 2019, cumulative update for SharePoint Enterprise Server 2013 (KB4484155)

This cumulative update package includes cloud hybrid search capability to SharePoint Server 2013. Learn about cloud hybrid search for SharePoint.

This cumulative update package fixes the issues that are described in the following Microsoft Knowledge Base (KB) articles:

- Description of the security update for SharePoint Foundation 2013: November 12, 2019 (KB4484157)
- Description of the security update for SharePoint Enterprise Server 2013: November 12, 2019 (KB4484151)

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

- When you open a lookup column's link in a new window or on a new tab, you receive a "404 Not Found" error message.

November 12, 2019, update for SharePoint Enterprise Server 2016 (KB4484147)

This update corrects some regional settings display names.

Description of the security update for SharePoint Enterprise Server 2016: November 12, 2019

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

- Removes the Hybrid Auditing feature from SharePoint Server 2016.
- Reduces the severity of certain upgrade sequence messages from WARNING to INFO. These messages indicate that the upgrade action doesn't have to make any changes because its database extension is currently not enabled in the database. For example, you will no longer see upgrade messages such as the following be labeled as warnings:

  "Ignoring upgrade sequence:

Microsoft.SharePoint.BusinessData.Upgrade.BdcDatabaseExtensionUpgradeSequence because related content database extension Microsoft.SharePoint.BusinessData.SharedService.BdcDatabaseExtension is not enabled."

- Fixes an issue that causes failures when you upload documents that contain links to very long URLs.
- Fixes an issue in which the web part displays no content when users visit a Content Search Web Part (CSWP) from the Google's page viewer or set the **AlwaysRenderOnServer** boolean in a Content Search Web Part (CSWP) to **True**.
- Fixes an issue in which the Product Version Timer Job fails on dedicated Search and Distributed Cache servers.
- Fixes an issue in which Publishing Cache items are missing page field data after the IIS app pool restarts.
- When a web application uses Default Configuration to configure SAML-based claims authentication by using Active Directory Federation Services (AD FS) and the people picker account resolution, users from an external trusted domain experience the following issues:
  - They cannot log on to a site.
  - They cannot be resolved by People Picker if they are set up by using ADFS and have "Email" as the identity claim.

This security update contains a fix for the following nonsecurity issue in Project Server 2016:

- In a Project Web App (PWA) project in which a proposed resource is replaced by a committed resource (or vice versa), existing assignments aren't replaced by the new resource. Instead, the assignments are lost.

Description of the security update for SharePoint Server 2019: November 12, 2019

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

- Corrects an issue in which certain HTTP headers are malformed in responses from SharePoint.
- Corrects an issue in which Publishing Cache items are missing page field data after the IIS app pool restarts.

- Corrects a "date out of range" exception when a user exports and then imports the site collection while Document ID feature is active.
- Fixes an issue in which the Product Version Timer Job fails on dedicated Search and Distributed Cache Servers.
- Fixes an issue in which the web part displays no content if users visit a Content Search Web Part (CSWP) from the Google's page viewer or set the **AlwaysRenderOnServer** boolean in a Content Search Web Part (CSWP) to **True**.
- When you have a Cloud Search Service Application (Cloud SSA) configured in SharePoint Server 2019, searches within the context of a list or library do not return any results.
- Consider the following scenario:
  - A user tries to access a host name site collection and is prompted to sign in.
  - A host name site collection is deleted while the user's session is still active.

  In this scenario, the user receives an "Access Denied" message on all subsequent attempts to access any other site collections by using that web application until they begin a new session.

  This issue is now resolved. The fix can be enabled on the server by running the following commands:

  ```
  $config = Get-SPSecurityTokenServiceConfig
  $config.WindowsModeIgnoreCache = $true
  $config.Update()
  ```
- When the Schedule Variance Percentage (SVP) or Cost Variance Percentage (CVP) earned value becomes very large, an overflow condition occurs. 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%**.
- After this update is installed, you can receive information about any type kind of completed queue jobs for a project when you use the new **GetAll()** method from a REST call.
- Consider the following scenario:
  - You create a new project in Project Web App.
  - When the schedule project detail page appears, the **Project Summary Task** is visible.

  In this situation, you cannot type in the **Task Name** field to create a new task.

- Consider the following scenario:

- As a timesheet user, you open your timesheet.
- On an assignment that has no actual work, you enter actual work on a given date.
- You save the timesheet.
- You change your mind, and you remove the actual work that you previously entered.
- You send the timesheet or status update for approval.
- The status manager approves the update.

In this scenario, when the assignment is viewed in Project Professional, it has an actual start date set even though you removed the actual work in the timesheet, and this also removed the actual start date. This fix correctly removes the assignment's actual start date in this situation.

Description of the security update for SharePoint Server 2019 Language Pack: November 12, 2019

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

- Corrects some regional settings display names.
- Fixes an issue in which you can't download results or reports in an eDiscovery site.