

What's in that patch? February 2021

Updated 2/11/2021

Table of Contents

What's in that patch? February 2021	1
Download Links.....	2
Fix Count	2
February 9, 2021, cumulative update for SharePoint Enterprise Server 2013 (KB4493209).....	2
Description of the security update for SharePoint Enterprise Server 2016: February 9, 2021 (KB4493195).....	2
Description of the security update for SharePoint Server 2019: February 9, 2021 (KB4493194)	3
February 9, 2021, update for SharePoint Server 2019 Language Pack (KB4493193)	5

Download Links

- <https://sharepointupdates.com/Patches>

Fix Count

SharePoint 2013	5
SharePoint 2016	9
SharePoint 2019	22

February 9, 2021, cumulative update for SharePoint Enterprise Server 2013 (KB4493209)

This security update resolves Microsoft SharePoint Spoofing Vulnerability, SharePoint Remote Code Execution Vulnerability, and SharePoint Information Disclosure Vulnerability. To learn more about these vulnerabilities, see the following security advisories:

- Microsoft Common Vulnerabilities and Exposures CVE-2021-1726
- Microsoft Common Vulnerabilities and Exposures CVE-2021-24071
- Microsoft Common Vulnerabilities and Exposures CVE-2021-24072
- Microsoft Common Vulnerabilities and Exposures CVE-2021-24066

Improvements and fixes

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

- Fixes RSS Viewer Web Part broken issues.

Description of the security update for SharePoint Enterprise Server 2016: February 9, 2021 (KB4493195)

This security update resolves a Microsoft SharePoint Spoofing Vulnerability, SharePoint Remote Code Execution Vulnerability, and SharePoint Information Disclosure Vulnerability. To learn more about these vulnerabilities, see the following security advisories:

- Microsoft Common Vulnerabilities and Exposures CVE-2021-1726
- Microsoft Common Vulnerabilities and Exposures CVE-2021-24071
- Microsoft Common Vulnerabilities and Exposures CVE-2021-24072
- Microsoft Common Vulnerabilities and Exposures CVE-2021-24066

Improvements and fixes

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

- While you browse Web Apps and Site Collections of unattached content databases by using the Backup and Restore feature in Central Administrator, selecting any Host Header Site Collection that includes port numbers would generate a blank screen.
- Fixes RSS Viewer Web Part broken issues.
- Fixes an issue in which the document URL in the callout ellipse in a document library is incorrectly displayed in a host-named site collection.
- Fixes an issue in which a user's information in a database is replaced by another user who has the same tp_Id in another database.

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

- No error message prompt is seen when a duplicated view is created in Project Web App.
- The start/finish date for a task is wrong after the task's assignment work is increased to > 0 and where the task is a milestone (duration is 0). This problem occurs after you install KB 4486753.

Known issues in this update

- **Issue 1**
If your customized SharePoint pages use the [SPWorkflowDataSource](#) or [FabricWorkflowInstanceProvider](#) user control, some functions on those pages may not work.
Resolution
To resolve this issue, see [KB5000640](#).
- **Issue 2**
The document URL in the callout ellipse in a document library is missing the DocID query string parameter if the Document ID feature is enabled.
Status
Microsoft is investigating this issue and will post more information in this article when a fix becomes available.
Workaround
To work around this issue, see [KB 5000957](#).

[Description of the security update for SharePoint Server 2019: February 9, 2021 \(KB4493194\)](#)

This security update resolves a Microsoft SharePoint Spoofing Vulnerability, SharePoint Remote Code Execution Vulnerability, and SharePoint Information Disclosure Vulnerability. To learn more about these vulnerabilities, see the following security advisories:

- [Microsoft Common Vulnerabilities and Exposures CVE-2021-1726](#)
- [Microsoft Common Vulnerabilities and Exposures CVE-2021-24071](#)
- [Microsoft Common Vulnerabilities and Exposures CVE-2021-24072](#)

- Microsoft Common Vulnerabilities and Exposures CVE-2021-24066

Improvements and fixes

This security update contains fixes for the following nonsecurity issues in SharePoint Server 2019:

- Fixes an issue in which a document library is empty after you leave it if you edit it in Quick Edit mode and then set a filter on the library's Managed Metadata column.
- Fixes an issue in which adding values to a multi-value Managed Metadata field does not work in Quick Edit mode.
- Fixes an issue in the English version of word breaker so that the feature can correctly break the "P1234 GRD" currency string.
- Fixes RSS Viewer Web Part broken issues.
- Fixes an issue in which an item display form generates an "access denied" message because of calculated date/time fields.
- Fixes an issue in which a user's information in a database is replaced by another user's information that has the same **tp_Id** in another database.
- Fixes an issue in which attachments from digitally signed email messages can't be saved to a document library.
- Fixes an issue in which SharePoint Designer doesn't work well against the site that disables the Wiki Home Page feature.
- Fixes an issue in which version comments cannot be saved when you upload files larger than 100 MB. After you apply this update, the following warning message will be displayed:

"Comments will not be saved with this file upload because the file is larger than 100 MB. After the file upload completes, you can check out and then check in the file to add a comment."

Note: To fix this issue completely, you have to install [KB 4493193](#) together with this update.

- Fixes the cursor focus issue that occurs when you edit the bullet list in multiple lines of a text field in Chrome browsers and Microsoft Edge based on Chromium.
- Fixes an issue in which the **Paste** ribbon button in the classic Rich Text Editor is disabled in modern browsers.
- Fixes an issue in which PeoplePicker does not resolve users from trusted domains if SharePoint uses Active Directory Federation Services (ADFS) and the default configuration.
- Fixes an issue in which SharePoint 2013 workflows are triggered recursively in lists that have managed metadata columns.

This security update also contains fixes for the following nonsecurity issues in Project Server 2019:

- Fixes accessibility issues in the **Pick Resource** feature (also seen in Project Web App as **Choose User**) dialog box because of an incorrect focus on the **OK** button. After you apply this update, the focus is set on the **Search Text Edit** field.
- The date range of the timescale on the Project Web App (PWA) Approvals page is off by one day if the user's time zone is set to a zone east of UTC. For example, UTC+2.
- In some situations, the Project Calculation Service (PCS) crashes while it opens a given project. The crash details that are logged in the SharePoint Unified Logging System (ULS) logs or in the Windows event logs resemble the following entry:

"The worker encountered a very serious error and will shutdown. Exception code was: 0xc0000005 (EXCEPTION_ACCESS_VIOLATION)."

- Ribbon buttons in the task management section (**View, Edit, Delete item**) in the task list are disabled for the tasks that are listed beyond the first page.

February 9, 2021, update for SharePoint Server 2019 Language Pack (KB4493193)

Improvements and fixes

- This update fixes an issue where version comments cannot be saved while you upload files larger than 100 MB. After you apply this update, the following warning message will be displayed:

"Comments will not be saved with this file upload because the file is larger than 100 MB. After the file upload completes, you can check out and then check in the file to add a comment."

Note: To fix this issue completely, you have to install [KB 4493194](#) together with this update.