What's in that patch? March 2020

Updated 4/23/2020

Table of Contents

Download Links

- https://sharepointupdates.com/Patches

Fix Count

SharePoint 2013	
March 10, 2020, cumulative update for Project Server 2013 (KB4484279)	7
SharePoint 2016	
4484272 - Description of the security update for SharePoint Enterprise Server 2016: March 10, 2020	10
4484275 - Description of the security update for SharePoint Enterprise Server 2016: March 10, 2020	1
SharePoint 2019	
4484277 - Description of the security update for SharePoint Server 2019 Language Pack: March 10, 2020	1
4484271 - Description of the security update for SharePoint Server 2019: March 10, 2020	14

Description of the security update for SharePoint Server 2013: March 10, 2020 (KB4484150)

This security update resolves a cross-site-scripting (XSS) vulnerability that exists if Microsoft SharePoint Server does not correctly sanitize a specially crafted web request to an affected SharePoint server. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2020-0893.

Description of the security update for SharePoint Foundation 2013: March 10, 2020 (KB4484282)

This security update resolves a vulnerability that occurs if SharePoint Server does not correctly sanitize a specially crafted request to an affected SharePoint server. To learn more about the vulnerability, see the following security advisories:

- Microsoft Common Vulnerabilities and Exposures CVE-2020-0795
- Microsoft Common Vulnerabilities and Exposures CVE-2020-0891
- Microsoft Common Vulnerabilities and Exposures CVE-2020-0894

Note To apply this security update, you must have the release version of Service Pack 1 for Microsoft SharePoint Foundation 2013 installed on the computer.

This security update contains the following improvement:

- Adding support for the SameSite cookie attribute to remain compatible with changes in how web browsers such as Chrome handle cookies.

Description of the security update for SharePoint Server 2013: March 10, 2020 (KB4475606)

This security update resolves a remote code execution vulnerability that exists in Microsoft Word software if the program does not correctly handle objects in memory. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2020-0850 and Microsoft Common Vulnerabilities and Exposures CVE-2020-0892.

Note To apply this security update, you must have the release version of Service Pack 1 for Microsoft SharePoint Server 2013 installed on the computer.

Description of the security update for SharePoint Foundation 2013: March 10, 2020 (KB4484124)

This security update resolves a remote code execution vulnerability that exists in Microsoft Word software if the program does not correctly handle objects in memory. To learn more

about thesvulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2020-0850 and Microsoft Common Vulnerabilities and Exposures CVE-2020-0892.

Note To apply this security update, you must have the release version of Service Pack 1 for Microsoft SharePoint Foundation 2013 installed on the computer.

4484272 - Description of the security update for SharePoint Enterprise Server 2016: March 10, 2020

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

- Adds support for the SameSite cookie attribute to remain compatible with changes in how web browsers such as Chrome handle cookies.
- When a list view uses **GroupBy** on a calculated **DateTime** field and includes a multi-valued lookup field, users can't expand any of the groups in the view. A "working on it" message appears where the group should be expanded, and an error dialog box appears. After this update is applied, the issue is fixed.
- After you create an enterprise custom field, the keyboard focus doesn't land on the next interactive element after you activate the **Select value** button.
- After you import an updated thesaurus into the Search Service Application, you may see a "something went wrong" error message when you search from the **Search** box.
- When you copy items that are declared as records through Windows Explorer, the copied items keep the record declaration status. This update fixes this issue.
- When a user opens multiple SharePoint links on multiple browser tabs, enters credentials in one of the tabs, and then refreshes the other tabs, the sign-in process doesn't occur seamlessly. Instead, the user is redirected to the root site and not actual site.
- Site collection level mappings do not occur for Default.aspx in each site's page library because the **SiteId** for Default.aspx is not generated correctly. After the fix is installed, the customized schema in site collection level will become active for default.aspx.

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

- In Project Web App (PWA), you can't edit in a lookup table's **Value** and **Description** columns while you use the Chrome browser.
- You edit a resource in Project Web App and use the Chrome browser. In this situation, although initials may exist for a work resource that's tied to a Windows user account,

the **Initials** field isn't populated and appears blank. Therefore, if the resource is saved, the blank initials are saved over the correct initials.

- You can't navigate through the tables on the **Approvals** and **Resource** pages by using a keyboard.

4484275 - Description of the security update for SharePoint Enterprise Server 2016: March 10, 2020

This security update replaces previously released update 4484255.

4484277 - Description of the security update for SharePoint Server 2019 Language Pack: March 10, 2020

This security update replaces previously released update 4484259.

4484271 - Description of the security update for SharePoint Server 2019: March 10, 2020

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

- Users navigate to a document library and open a Links list in Job Access With Speech (JAWS) by using a keyboard shortcut (Alt+F7) to see all links on the page.
  Every document in the library contains the **Open Menu** link to open the **Edit Control Block (ECB)** menu. Therefore, it is not possible to know which document belongs to which link. This update fixes the issue.

  Note To fix this issue, you have to install update 4484277 together with this update.
- Fixes an issue that prevents users from switching content type when they create items in a list.
- Removes the **Link** command from the **New** menu in custom lists when content types are enabled.

  Note To fix these issues, you have to install update 4484277 together with this update.

- When you have a hyperlink column as the first column in your view, and you have a very long navigation list, the edit box for the hyperlink column in Quick Edit opens underneath the navigation pane. This makes it difficult to edit or add a value in the edit box.
- Fixes an issue in which creating a site master fails if multiple authentication methods are used for the web application.

- When you use the Edge browser, CSPReporting.aspx is requested multiple times during page loading when you access modern pages. This update fixes this issue.
- Screen readers such as Narrator don't show an "alt" text entry for icons of **Search** buttons when you bulk edit multiple resources.
- After you import an updated thesaurus into the Search Service Application, you may see a "something went wrong" error message when you search from the "Search Box".
- When you use the Finnish locale version, the dates for Blog and List items don't render correctly. This update fixes this issue.
- When you copy items that are declared as records through Windows Explorer, the copied items keep the record declaration status. This update fixes this issue.
- Fixes an issue that causes content deployment jobs to fail if a document library contains a file that has multiple versions.

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

- After you edit a project in Project Web App, it may take a long time to save the project. This is especially true if there are many custom field values. This causes slower publishing, check-in jobs, and other related actions.
- Editing a project in Project Web App or approving status updates uses the Project Calculation Service (PCS). In some situations, PCS crashes while it closes the given project. The crash detail is logged in the Unified Logging System (ULS) logs, and it resembles the following:

  "The worker encountered a very serious error and will shut down. Exception code was: 0xc0000005 (EXCEPTION_ACCESS_VIOLATION)."
- Consider the following scenario:
  - You have an enterprise resource custom field.
  - You edit a resource and assign a value to the field.
  - You delete the enterprise resource field.
  - You edit the resource, and save your changes.

  In this scenario, the process fails, and you receive the following error message:

  "Unknown error has occurred"