What's in that patch? January 2022

Updated 1/30/2022

Table of Contents

Download Links

- https://sharepointupdates.com/Patches

Fix Count

SharePoint 2013	4
SharePoint 2016	10
SharePoint 2019	22

Description of the security update for SharePoint Foundation 2013: January 11, 2022 (KB5002127)

To better protect and strengthen the security of SharePoint, SharePoint now restricts access to its Web.config files. Users cannot access Web.config files unless they're local administrators, farm administrators, or managed by SharePoint. This change does not impact standard SharePoint functionality. For more information about this improvement, see Permissions of Web.config files are restricted in SharePoint Server (KB5010126).

Description of the security update for SharePoint Foundation 2013: January 11, 2022 (KB5002129)

This security update resolves a Microsoft Office remote code execution vulnerability. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2022-21840.

Description of the security update for SharePoint Enterprise Server 2013: January 11, 2022 (KB5001995)

This security update resolves a Microsoft Office remote code execution vulnerability. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2022-21840.

Description of the security update for SharePoint Enterprise Server 2013: January 11, 2022 (KB5002102)

This security update resolves a Microsoft Office remote code execution vulnerability. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2022-21840.

Description of the security update for SharePoint Enterprise Server 2016: January 11, 2022 (KB5002113)

This security update resolves a Microsoft Word remote code execution vulnerability, Microsoft Office remote code execution vulnerability, and Microsoft SharePoint Server remote code execution vulnerability. To learn more about the vulnerabilities, see the following security advisories:

Microsoft Common Vulnerabilities and Exposures CVE-2022-21842

Microsoft Common Vulnerabilities and Exposures CVE-2022-21840

Microsoft Common Vulnerabilities and Exposures CVE-2022-21837

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

- To better protect and strengthen the security of SharePoint, SharePoint now restricts access to its Web.config files. Users cannot access Web.config files unless they're local administrators, farm administrators, or managed by SharePoint. This change does not impact standard SharePoint functionality. For more information about this improvement, see Permissions of Web.config files are restricted in SharePoint Server (KB5010126).
- Fixes an issue in which a double URL encoding occurs when you try to open documents in a client application in Google Chrome from Mac devices.
- Fixes an issue in which an error occurs when you share a folder in a list under a subsite.
- Fixes an issue in which the Word Automation Services assembly (Sword.dll) is not updated to the expected version.
- Fixes an issue in which selecting the **New** button in the form library opens a dialog box to upload files instead of opening the InfoPath client application.

This security update also provides security improvements for Project Server 2016.

Description of the security update for SharePoint Enterprise Server 2016: January 11, 2022 (KB5002118)

This security update resolves a Microsoft Office remote code execution vulnerability and Microsoft Word remote code execution vulnerability. To learn more about the vulnerabilities, see the following security advisories:

Microsoft Common Vulnerabilities and Exposures CVE-2022-21842

Microsoft Common Vulnerabilities and Exposures CVE-2022-21840

Description of the security update for SharePoint Server 2019: January 11, 2022 (KB5002109)

This security update resolves a Microsoft Office remote code execution vulnerability. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2022-21840.

This security update contains fixes for the following nonsecurity issues:

- Fixes an issue in which the Content Deployment feature cannot publish incremental changes.
- Fixes an issue in which the multi-value properties do not show the required information banner and do not enforce required data in the modern view of a document library.
- Fixes an issue in which the information pane always scrolls to the bottom when you select an item detail in a document library.
- Fixes some layout issues on the modern search result page in the Hebrew language.
- Fixes an issue in which the Modern Document Library web part crashes when you upload a file without an extension.
- Fixes an issue in which the hidden nodes of the left navigation pane are shown in the modern team site when the Publishing feature is enabled.

Description of the security update for SharePoint Server 2019 Language Pack: January 11, 2022 (KB5002108)

This security update resolves a Microsoft Office remote code execution vulnerability and Microsoft SharePoint Server remote code execution vulnerability. To learn more about the vulnerabilities, see the following security advisories:

Microsoft Common Vulnerabilities and Exposures CVE-2022-21840

Microsoft Common Vulnerabilities and Exposures CVE-2022-21837

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

- To better protect and strengthen the security of SharePoint, SharePoint now restricts access to its Web.config files. Users cannot access Web.config files unless they're local administrators, farm administrators, or managed by SharePoint. This change does not impact standard SharePoint functionality. For more information about this improvement, see Permissions of Web.config files are restricted in SharePoint Server (KB5010126).
- Removes unnecessary stored procedure executions that can cause SQL Server deadlocks when multiple apps are present on a page together with a high user load.
- Fixes an issue in which you cannot copy and paste list items in quick edit mode by using a modern browser.

- Improves the page rendering performance.
- Fixes an issue in which selecting the **New** button in the form library opens a dialog box to upload files instead of opening the InfoPath client application.
- Fixes an issue in which selecting an existing form in a form library that is set to OpenInClient does not start the InfoPath client application, and you receive the following error message:

  > This action couldn't be performed because Office doesn't recognize the command it was given.

This security update also contains fixes for the following nonsecurity issues in SharePoint Server 2019. To fix these issues completely, you have to install KB 5002108 together with this update.

- Fixes an issue in which the Content Deployment feature cannot publish incremental changes.
- Fixes an issue in which the multi-value properties do not show the required information banner and do not enforce required data in the modern view of a document library.
- Fixes an issue in which the information pane always scrolls to the bottom when you select an item detail in a document library.
- Fixes some layout issues on the modern search result page in the Hebrew language.
- Fixes an issue in which the Modern Document Library web part crashes when you upload a file without an extension.
- Fixes an issue in which the hidden nodes of the left navigation pane are shown in the modern team site when the Publishing feature is enabled.

This security update fixes the following nonsecurity issue in Project Server 2019:

- Fixes an issue in which you cannot filter resources by using the options under the **Outline** menu in the Build Team functionality.

This security update also provides some security improvements for Project Server 2019.