What's in that patch? November 2020

Table of Contents

Download Links

- https://sharepointupdates.com/Patches

Fix Count

SharePoint 2013	5
SharePoint 2016	6
SharePoint 2019	14

Description of the security update for SharePoint Foundation 2013: November 10, 2020

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see the following security advisories:

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-16979](#)
- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17015](#)
- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17017](#)
- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17061](#)

Description of the security update for SharePoint Enterprise Server 2013: November 10, 2020

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see [Microsoft Common Vulnerabilities and Exposures CVE-2020-17016](#) and [Microsoft Common Vulnerabilities and Exposures CVE-2020-17060](#).

Description of the security update for SharePoint Enterprise Server 2016: November 10, 2020

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see the following security advisories:

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-16979](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17015](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17016](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17017](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17060](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17061](#)

Description of the security update for SharePoint Server 2019: November 10, 2020

This security update resolves vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. To learn more about these vulnerabilities, see the following security advisories:

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-16979](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17015](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17016](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17017](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17060](#)

- [Microsoft Common Vulnerabilities and Exposures CVE-2020-17061](#)

November 10, 2020, update for SharePoint Server 2019 Language Pack (KB4486715)

This update contains the following fixes. To fix these issues completely, you have to install [KB 4486714](#) together with this update:

- Fixes an issue in which the Date Picker doesn't render in the **Modern Item Properties** pane in document libraries.

- Fixes an issue in which the role of the **Theme** pane is not announced, and the position is announced by the screen reader.

- Fixes an issue in which the incorrect **Theme** pane position is announced by the screen reader.

- Fixes an issue in which a tooltip isn't provided for **Add a link** and **More option** buttons.

- Fixes an issue in which the Activity Web Part doesn't generate the correct URLs if the site is hosted on a non-default port.

- Fixes an issue in which search results aren't announced by screen reader on an available search edit field after activating "+ add web part."

- Fixes an issue in which elements with an Aria role that require the child role aren't contained by them in a TeamSite page under the News and Activity Web Part.

- Fixes an issue in which the Aria label isn't defined for the **Cancel** button (X) when you search for various Web Parts in the canvas toolbox.