What's in that patch? September 2019

Updated 9/21/2019

Table of Contents

Download Links

- http://www.toddklindt.com/sp2013builds
- http://www.toddklindt.com/sp2016builds
- https://sharepointupdates.com/Patches

Fix Count

SharePoint 2013	
Description of the security update for SharePoint Foundation 2013: September 10, 2019	1
Description of the security update for SharePoint Foundation 2013: September 10, 2019	7
SharePoint 2016	
Description of the security update for SharePoint Enterprise Server 2016: September 10, 2019 (4475590)	7
Description of the security update for SharePoint Enterprise Server 2016: September 10, 2019 (4475594)	2
SharePoint 2019	
Description of the security update for SharePoint Server 2019: September 10, 2019	11
Description of the security update for SharePoint Server 2019 Language Pack: September 10, 2019	1

Description of the security update for SharePoint Foundation 2013: September 10, 2019

This security update resolves an elevation of privilege vulnerability that exists in Microsoft SharePoint. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2019-1260.

Description of the security update for SharePoint Foundation 2013: September 10, 2019

This security update resolves a remote code execution vulnerability that exists in Microsoft SharePoint if the software does not check the source markup of an application package. To learn more about the vulnerability, see the following security advisories:

- Microsoft Common Vulnerabilities and Exposures CVE-2019-1257
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1259
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1260
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1261
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1262
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1295
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1296

Description of the security update for SharePoint Enterprise Server 2016: September 10, 2019 (4475590)

This security update resolves a remote code execution vulnerability that exists in Microsoft SharePoint if the software does not check the source markup of an application package. To learn more about this vulnerability, see the following security advisories:

- Microsoft Common Vulnerabilities and Exposures CVE-2019-1257
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1260
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1261
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1295
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1296

This security update contains the following improvements in SharePoint Enterprise Server 2016:

- Uninstalling an app when the second stage recycle bin is cleared now occurs only if no instances of the app currently exist.

- With this update, in-place searches will now look for only results within the currently viewed folder. This greatly improves the search experience within a folder in large libraries that have files that spread across multiple folders.

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

- When you attach a content database from a previous version of SharePoint Server to SharePoint Server 2016, any existing "Table of Contents" web parts in that database always have the "Show content from starting location" setting enabled after the upgrade. This update fixes this issue by preserving the original setting during the upgrade.

- You randomly receive a FedAuth cookie even though you have enabled Windows Authentication as the only authentication provider on your web application.

  Note To fix this issue completely, you must install KB 4475594 together with this update.

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

- Users can now add tasks while editing a project in the Schedule view when the **Project Summary Task** option is selected.

- You can now receive information about any type kind of completed queue jobs for a project when you use the new **GetAll()** method from a REST call.

- When the Schedule Variance Percentage (SVP) earned value becomes very large, it causes an overflow condition that prevents Project Web App (PWA) project views from loading. The SVP value now has a lower limit of **-100%** and upper limit of **100%**.

Description of the security update for SharePoint Enterprise Server 2016: September 10, 2019 (4475594)

This security update resolves an elevation of privilege vulnerability that exists in Microsoft SharePoint. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2019-1260.

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

- You randomly get a FedAuth cookie even though you have enabled Windows Authentication as the only authentication provider on your web application.

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

This security update resolves a remote code execution vulnerability that exists in Microsoft SharePoint if the software does not check the source markup of an application package. To learn more about this vulnerability, see the following CVE descriptions:

- Microsoft Common Vulnerabilities and Exposures CVE-2019-1257
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1260
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1261
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1295
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1296

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

- When file paths on file shares are longer than the default Windows supported path length (260 characters), files are crawled without access control list (ACL) information.

- Installing a SharePoint Server 2019 solution on a multi-server farm is an unreliable process and will not necessartily succeed.

- When you attach a content database from a previous version of SharePoint Server to SharePoint Server 2019, existing "Table of Contents" web parts in that database would always have the "Show content from starting location" setting enabled after the upgrade. This update fixes this issue by preserving the original setting during upgrade.

- Through the client-side object model (CSOM), the TaskLink ProjUid property for an external task returns the ID of its own project instead of the ID of the project that the

task refers to. This update adds the ExternalProjectUid and ExternalTaskUid properties to the Task class to fix this issue.

- Loading a timesheet is very slow and may take one minute or more.

- Project Server Interface (PSI) API calls that require the permission of a farm administrator fail for users who are farm administrators but not server administrators.

Description of the security update for SharePoint Server 2019 Language Pack: September 10, 2019

This security update resolves an elevation of privilege vulnerability that exists in Microsoft SharePoint. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2019-1260.