What's in that patch? June 2019

Updated 6/12/2019

Table of Contents

What's in that patch? June 2019 1

Download Links 1

Fix Count 1

Description of the security update for SharePoint Enterprise Server 2013: June 11, 2019 2

Description of the security update for SharePoint Foundation 2013: June 11, 2019 2

Description of the security update for SharePoint Enterprise Server 2016: June 11, 2019 2

Description of the security update for SharePoint Server 2019: June 11, 2019 4

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 Enterprise Server 2013: June 11, 2019	1
Description of the security update for SharePoint Foundation 2013: June 11, 2019	3
SharePoint 2016	
Description of the security update for SharePoint Enterprise Server 2016: June 11, 2019	15
SharePoint 2019	
Description of the security update for SharePoint Server 2019: June 11, 2010	13

Description of the security update for SharePoint Enterprise Server 2013: June 11, 2019

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 that's made to an affected SharePoint server. To learn more about the vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2019-1031.

Description of the security update for SharePoint Foundation 2013: June 11, 2019

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:

- Microsoft Common Vulnerabilities and Exposures CVE-2019-1033
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1034
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1036

Description of the security update for SharePoint Enterprise Server 2016: June 11, 2019

This security update resolves a cross-site-scripting (XSS) vulnerability that exists when Microsoft SharePoint Server does not correctly sanitize a specially crafted web request to an affected SharePoint server. This update also resolves a remote code execution vulnerability that exists in Microsoft Word software when it fails to correctly handle objects in memory. To learn more about the vulnerabilities, see the following:

- Microsoft Common Vulnerabilities and Exposures CVE-2019-1031
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1032
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1033
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1034
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1036

Contains the following improvements in SharePoint Server 2016:

- Adds the new Japanese era name in the Japanese word breaker to make sure that the new era name can be correctly broken during a search.

- Spanish is now an option among the search language preference in the SharePoint classic search if users from Argentina and other countries from South America set Spanish as their language preferences in the browser.

Contains fixes for the following nonsecurity issues in SharePoint Server 2016:

- When you start crawling for some content that has many links, the crawl fails because the number of links exceeds a search limitation. After multiple failures, the content is deleted unexpectedly. After this update is installed, you can set the maximum number of links that are sent to the index by using the **ContentPIMaxNumLinks** property. To set **ContentPIMaxNumLinks** (for example, to 10,000), you can use commands that resemble the following:

- `$ssa = Get-SPEnterpriseSearchServiceApplication`
- `$ssa.SetProperty("ContentPIMaxNumLinks", 10000)`
  `$ssa.Update()`
- Assume that you enable McAfee Security for SharePoint Server 2016. When you access a large OneNote file that has an attachment in SharePoint Server 2016, an application pool crashes intermittently.

- You experience errors when you create a document that is set to use the **DD/MM/YYYY** date format. This issue may occur if users configure their My Site Profile information to use their local regional settings, such as **French/Luxembourg**.

- The SharePoint file plan report doesn't generate the hyperlink for a URL that contains special characters, such as white spaces.

- Assume that you view a Datasheet View on a list by using the Internet Explorer browser. You try to paste a cell that has multiple lines of text from an Excel worksheet into a field that uses the **Multiple lines of text** type option in the Datasheet view. When you try to paste the cell, you receive an error message, and the paste operation fails.

Contains fixes for the following nonsecurity issues in Project Server 2016:

- Adds the **PublishSummary** method for the ProjectCollection class in the client-side object model (CSOM) so that project-level fields on a project can be published independently from the entire project.

- Updating resources through the client-side object model (CSOM) takes a long time or causes a time-out.

- When you update a task in a timesheet, after the status update is applied to the project, in Project you may observe unexpected results to the resource assignment. For example, the custom remaining work contour has changed to **Flat**. Or, the finished date of the assignment on a fixed duration task is earlier than expected.

Description of the security update for SharePoint Server 2019: June 11, 2019

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. It also resolves a remote code execution vulnerability that exists in Microsoft Word software if the program fails to correctly handle objects in memory. To learn more about the vulnerabilities, see the following:

- Microsoft Common Vulnerabilities and Exposures CVE-2019-1031
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1032
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1033
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1034
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1035
- Microsoft Common Vulnerabilities and Exposures CVE-2019-1036

Contains the following improvements:

- Adds the new Japanese era name in the Japanese word breaker to make sure that the new era name can be correctly broken when during a search.

- Spanish is now an option among the search language preference in the SharePoint classic search if users from Argentina and other countries from South America set Spanish as their language preferences in the browser.

Contains fixes for the following nonsecurity issues:

- In some circumstances, if you delete a few views that are associated with custom fields that support multi-value selection from a lookup table in the database, and then you run the **Repair-SPProjectWebInstance** cmdlet, you find that the first view isn't generated in the database.

- Files that have Information Rights Management (IRM) protection in Modern UI are blocked from being uploaded to a document library.

- Existing folders can be marked as special folders only if they are empty. Now, folders that have existing content can be used.

- Certain calendar picker options for setting **CalendarWeekRule** update the value incorrectly.

- After you install the January 2019 update, the "Resources" web part is removed from the Central Administration homepage. This update corrects the issue and restores the "Resources" web part to the Central Administration homepage.