Security Advisory 2020-025

Microsoft Sharepoint – RCE in TypeConverters

May 6, 2020 — v1.0

TLP:WHITE

History:

- *06/05/2020 — v1.0 – Initial publication*

Summary

On the 14th of April 2020, Microsoft released several security advisories for vulnerabilities affecting Microsoft Sharepoint [1]. On the 29th of April 2020, Zero Day Initiative released a blog post [2] providing details on one of these vulnerabilities (CVE-2020-0932 [3]).

This vulnerability allows authenticated users to execute arbitrary code on a SharePoint server in the context of the service account. To successfully exploit the vulnerability, attacker needs some specific permission (*Add or Customize Pages*). However, in the default configuration of SharePoint this permission is given to any user as any user can create its own SharePoint site.

Technical Details

The vulnerability is due to improper restriction on available types for properties when the XML configuration of WebParts is parsed. An attacker can use this lack of restriction to convert payload into executable object on the server with the right of the service account.

A full description of the vulnerability is available on Zero Day Initiative blogpost [2].

Products Affected

- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Server 2019

Recommendations

Microsoft has released patches for this vulnerability [3]. It is strongly advised to apply the security update from Microsoft to fix this vulnerability as soon as possible.

It is also recommended to monitor suspicious access to `/_vti_bin/WebPartPages.asmx` web page, as is it used as entry point for the attack.

Workarounds

In order to prevent exploitation of the vulnerability, it is recommended to ensure that users do not have the possibility to create a site, add or customise page if not explicitly needed. It is important to note that users with `Read` permission level **can create site** on the SharePoint server.

References

[1] https://support.microsoft.com/en-us/help/4484299/security-update-for-sharepoint-server-2016-april-14-2020

[2] https://www.thezdi.com/blog/2020/4/28/cve-2020-0932-remote-code-execution-on-microsoft-sharepoint-using-typeconverters

[3] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0932