CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-030

Microsoft Sharepoint – RCE in ASP.Net Web Controls

June 19, 2020 — v1.0

TLP:WHITE

History:

- *19/06/2020 — v1.0 – Initial publication*

Summary

On the 6th of June 2020, Microsoft released a security advisory for a vulnerability affecting Microsoft Sharepoint [1] identified as CVE-2020-1181. On the 17th of June 2020, Zero Day Initiative released a blog post [2] providing a proof of concept on how to exploit the vulnerability [3].

This vulnerability allows authenticated users to execute arbitrary code on a SharePoint server with privileges of the service account. An attacker may create and call a specific crafted page to successfully exploit the vulnerability. In the default configuration of SharePoint, the necessary permission is given to any user as any user can create its own SharePoint site.

Technical Details

The vulnerability is due to improper identification and filtering of unsafe ASP.NET web controls. An attacker can use this lack of restriction to convert a payload into an executable object on the server with the permissions 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 2010 Service Pack 2
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Server 2019

Recommendations

Microsoft has released security updates for the affected products regarding this vulnerability [1]. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles processing of created content.

It is strongly recommended to apply the security updates from Microsoft as soon as possible.

Workarounds

There are no known workarounds.

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1181

[2] https://www.thezdi.com/blog/2020/6/16/cve-2020-1181-sharepoint-remote-code-execution-through-web-parts

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1181