CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-050

Microsoft Sharepoint – Remote Code Execution Vulnerability

October 19, 2020 — v1.0

TLP:WHITE

Summary

On the 13th of October 2020, Microsoft released a security advisory for a vulnerability affecting Microsoft Sharepoint identified as CVE-2020-16952 [1]. Since then, security specialist Steven Seeley released a proof of concept on how to exploit the vulnerability [2]. Also, a Metasploit module exploiting CVE-2020-16952 has been published and contains remote check logic as well as supplementary exploitation details.

Successful exploitation of this vulnerability would allow an attacker to run arbitrary code and carry out security actions in the context of the SharePoint application pool and the SharePoint server farm account. The issue results from the lack of proper validation of user-supplied data which can result in a server-side code include. Authentication is however required to exploit this vulnerability.

Technical Details

The vulnerability is due to validation issue in user-supplied data. This vulnerability can be exploited when a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The bug is exploitable by an authenticated user with page creation privileges, which is a standard permission in SharePoint, and allows the leaking of an arbitrary file, notably the application's `web.config` file, which can be used to trigger remote code execution (RCE) via .NET deserialisation. The released security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.

A full description of the vulnerability is available on Rapid7 analysis [3].

Products Affected

- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- SharePoint Online as part of Office 365 is not affected.

Recommendations

Microsoft has released patches for this vulnerability [1]. 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 for the exploit variant by identifying HTTP headers containing the string `runat="server"`, as well as auditing SharePoint page creations.

Workarounds

Microsoft has not identified any mitigation factors and workarounds for this vulnerability.

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16952

[2] https://srcincite.io/pocs/cve-2020-16952.py.txt

[3] https://attackerkb.com/topics/4yGC4tLK2x/cve-2020-16952-microsoft-sharepoint-remote-code-execution-vulnerabilities#rapid7-analysis