Security Advisory 2022-010

RCE Vulnerabilities in Microsoft Sharepoint and DNS

February 9, 2022 — v1.0

TLP:WHITE

History:

- *09/02/2022 — v1.0 – Initial publication*

Summary

On February 8, Microsoft released 51 new patches addressing CVEs in various Microsoft products [1]. Two of them are categorised as significant (rating: High) vulnerabilities with the CVSS score of 8.8. The first vulnerability identified as `CVE-2022-22005` [2] is affecting Microsoft SharePoint Server, and it can lead to remote code execution in case the attacker is authenticated and possess the permissions for page creation. The second vulnerability identified as `CVE-2022-21984` [3] is affecting the Microsoft DNS Server, and it can lead also to remote code execution if the DNS server has the dynamic updates enabled.

No proof-of-concept or ongoing exploitation of these vulnerabilities are have been observed yet, however, it is highly recommended to apply the patches as soon as possible.

Technical Details

The vulnerability `CVE-2022-22005` could allow an authenticated user to execute any arbitrary .NET code on the server under the context and permissions of the service account of SharePoint Web Application. An attacker would need *Manage Lists* permissions to exploit this. By default, authenticated users are able to create their own sites and, in this case, the user will be the owner of this site and will have all necessary permissions [4].

CVE-2022-21984 fixes a remote code execution bug in the Microsoft DNS server. The server is only affected if dynamic updates are enabled, but this is a relatively common configuration. With this setup, an attacker could completely take over the DNS server and execute code with elevated privileges. Since dynamic updates are not enabled by default, this does not get a Critical rating. However, if the DNS servers do use dynamic updates, this vulnerability should be treated as Critical [4].

Affected Products

CVE-2022-22005

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016

CVE-2022-21984

- Windows 10 Version 21H2 for 32-bit, x64 and AMR64 -based Systems
- Windows 11 for x64 and ARM64-based Systems
- Windows Server, version 20H2 (Server Core Installation)
- Windows 10 Version 32-bit, x64 and AMR64 -based Systems
- Windows Server 2022 Azure Edition Core Hotpatch
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows 10 Version 21H1 for 32-bit, x64 and AMR64 -based Systems
- Windows 10 Version 1909 for 32-bit, x64 and AMR64 -based Systems

Recommendations

Microsoft recommends to apply the Security Updates detailed in [2] and [3].

References

[1] https://msrc.microsoft.com/update-guide/en-us

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22005

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984

[4] https://www.zerodayinitiative.com/blog/2022/2/8/the-february-2022-security-update-review