CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-047

RCE Vulnerability in Microsoft MSHTML

September 17, 2021 — v1.1

TLP:WHITE

History:

- *08/09/2021 — v1.0 – Initial publication*
- *17/09/2021 — v1.1 – Update with information about a new patch*

Summary

On 7th of September 2021, Microsoft released information about a vulnerability (CVE-2021-40444) in MSHTML that affects Microsoft Windows that could be exploited by sending specially-crafted Microsoft Office documents to potential victims [1]. The severity of this vulnerability is **high**, with CVSSv3 Score 8.8.

However, the attack is prevented by Protected View mode or Application Guard for Office 365, if Microsoft Office runs with the default configuration. The attacker would then have to mislead the user to open the malicious document and enable the active content.

Microsoft is aware of targeted attacks that attempt to exploit this vulnerability by using specially-crafted Microsoft Office documents.

On the 14th of September, Microsoft has released security updates to address this vulnerability [1].

Technical Details

An attacker could craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. Once opened, the document will load the Internet Explorer engine to render a remote web page from the threat actor. Malware is then downloaded by using a specific ActiveX control in the web page. Executing the threat is done using a trick called *Cpl File Execution* referenced in Microsoft's advisory [2].

Products Affected

Windows 7, 8.1 and 10 (including versions 2004), Windows Server 2008, 2016, 2019, 2022 and Windows Server Core versions. For more specific type and version please check [1].

Recommendations

CERT-EU recommends to apply the patches released on September 2021 Patch Tuesday as soon as possible.

Additionally, systems with active Microsoft's Defender Antivirus and Defender for Endpoint (build 1.349.22.0 and above) benefit from protection against attempts to exploit CVE-2021-40444. Moreover, by default, Microsoft Office opens documents from the internet in Protected View or Application Guard for Office both of which prevent the current attack.

Workarounds and Mitigations

Disabling the installation of all ActiveX controls in Internet Explorer mitigates this attack. This can be accomplished for all sites by updating the registry. Previously-installed ActiveX controls will continue to run, but do not expose this vulnerability.

Please follow the instructions from the advisory to disable ActiveX controls [1]. This sets the `URLACTION_DOWNLOAD_SIGNED_ACTIVEX (0x1001)` and `URLACTION_DOWNLOAD_UNSIGNED_ACTIVEX (0x1004)` to `DISABLED (3)` for all internet zones for 64-bit and 32-bit processes. New ActiveX controls will not be installed. Previously-installed ActiveX controls will continue to run.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

[2] https://www.bleepingcomputer.com/news/security/microsoft-shares-temp-fix-for-ongoing-office-365-zero-day-attacks/