0.1 CVE-2020-24086

According to Microsoft[1] CVE-2021-24086 is a denial of service vulnerability with a CVSS:3.0 score of 7.5 / 6.5, that is a base score metrics of 7.5 and a temporal score metrics of 6.5. The vulnerability affects all supported versions of Windows and Windows Server. According to an accompanied blog post published by Microsoft [3] at the same time as the patch was released, details that the vulnerable component is the Windows TCP/IP implementation, and that the vulnerability revolves around IPv6 fragmentation. The Security Update guide and the blog post also present a workaround that can be used to temporarily mitigate the vulnerability by disabling IPv6 fragmentation.

0.1.1 Public information

Due to the Microsoft Active Protetions Program (MAPP)[2] security software providers are given early access to vulnerability information. This information often include Proof of Concept (PoC)s Microsoft has the MAPP

0.1.2 Patch diffing

0.1.3 Root-cause analysis

0.1.4 Triggering the vulnerability