Security Advisory 2020-014

SMBv3 – Critical Remote Code Execution Vulnerability

March 13, 2020 — v1.1

TLP:WHITE

History:
- 11/03/2020 — v1.0 – Initial publication
- 13/03/2020 — v1.1 – Update with information about the patch available

Summary

On the 10th of March 2020, Microsoft released a security advisory for a remote code execution vulnerability affecting Microsoft Server Message Block 3.1.1 (SMBv3) protocol [1]. An unauthenticated attacker who successfully exploited the vulnerability could execute code on a target SMB Server or SMB Client. The vulnerability is referenced as CVE-2020-0796.

Microsoft re-released this month’s Patch Tuesday security update to fix this vulnerability [4].

Technical Details

The vulnerability can be exploited in two different ways:
- by sending a specially crafted packet to a targeted SMBv3 server,
- by convincing a user to connect to a malicious SMBv3 server.

Microsoft has not disclosed the technical information on the vulnerability, however, based on the workaround provided by Microsoft [1], the vulnerability appears to be linked to handling of compressed data packets.

FortiGuard Labs also released an IPS rule describing the vulnerability as being related to a Buffer Overflow [2]. According to FortiGuard Labs, the vulnerability is due to an error when the vulnerable software handles a maliciously crafted compressed data packet.

More technical details have now been provided in [5].
Products Affected

- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

Recommendations

Microsoft has released a patch for this vulnerability [4]. It is strongly advised to apply the security update KB4551762 from Microsoft to fix this vulnerability as soon as possible.

References