Security Advisory 2020-003

Critical Vulnerabilities in Microsoft Windows

January 15, 2020 — v1.0

TLP:WHITE

History:

• 15/01/2020 — v1.0 – Initial publication

Summary

Several critical vulnerabilities affecting Microsoft Windows were patched on 14th of January 2020, as part of the regular patch Tuesday [1]. Some the vulnerabilities are quite critical, so it is extremely important to apply the patches as soon as possible.

A vulnerability identified as CVE-2020-0601 is affecting the Microsoft Windows CryptoAPI enabling a malicious software to appear as authentically signed by a trusted or trustworthy organisation. Other vulnerabilities, identified as CVE-2020-0609, CVE-2020-0610, and CVE-2020-0611 respectively, are affecting the Windows Remote Desktop Server and Client, and could lead to remote code execution [2].

Technical Details

The vulnerability CVE-2020-0601 exists in the way the Microsoft Windows CryptoAPI (crypt32.dll) validates Elliptic Curve Cryptography certificates [1]. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.

The vulnerabilities CVE-2020-0609 and CVE-2020-0610 affecting the Windows Remote Desktop Gateway Server could allow remote code executions by an unauthenticated attacked thanks to specially crafted requests. These vulnerabilities do not require user interaction [3, 4]. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The vulnerability CVE-2020-0611 affecting the Windows Remote Desktop Client could allow a remote code execution on the client computer. To do so, an attacker needs to have control of a server and convince a user to connect to it. Then, the attacker could execute arbitrary code on the computer of the connecting client [5].
Affected Products

An overview of the affected products is presented below. For detailed list of affected versions, please consult [1, 3, 4, 5].

Microsoft Windows CryptoAPI vulnerability - CVE-2020-0601 [1]:
- Windows 10 for 32-bit Systems and x64-based Systems
- Windows Server 2016 and 2019

Windows Remote Desktop Server vulnerabilities - CVE-2020-0609, CVE-2020-0610 [3, 4]:

Windows Remote Desktop Client vulnerability - CVE-2020-0611 [5]:
- Windows 10 for 32-bit Systems and x64-based Systems
- Windows 8.1 for 32-bit and x64-based Systems
- Windows 7 for 32-bit and x64-based Systems (SP1)
- Windows Server 2008 R2 for Itanium-based and x64-based Systems (SP1)

Recommendations

Microsoft has released patches to address these vulnerabilities. It is highly recommended to apply these critical patches as soon as possible, first on critical systems, internet-facing systems and network servers, and then on other affected assets.

NSA has issued also its recommendations for mitigating actions [6], which may be used as a guideline if enterprise-wise automatic patching is not possible.

References