Security Advisory 2020-048

Critical Vulnerability in Microsoft Windows TCP/IP Stack

October 14, 2020 — v1.0

TLP:WHITE

History:

- *14/10/2020 — v1.0 – Initial publication*

Summary

On 13th of October 2020, Microsoft released several security advisories to address security vulnerabilities. One of the reported vulnerabilities, affects Windows TCP/IP stack. An attacker who successfully exploits this vulnerability could gain the ability to execute code on the target server or client [1].

Technical Details

The vulnerability was dubbed *Bad Neighbor* because it is located within an ICMPv6 Neighbor Discovery Protocol, while using the Router Advertisement type. It has received the CVE-2020-16898 and a CVSS Score of 9.8. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.

This remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets that use Option Type 25 (Recursive DNS Server - RDNSS - Option) and a length field value that is even. In this Option, the length is counted in increments of 8 bytes, so an RDNSS option with a length of 3 should have a total length of 24 bytes.

The option itself consists of five fields: Type, Length, Reserved, Lifetime, and Addresses of IPv6 Recursive DNS Servers. The first four fields have a length of 8 bytes, but the last field can contain a variable number of IPv6 addresses, which are 16 bytes each. As a result, the length field should always be an odd value of at least 3, per RFC 8106. When an even length value is provided, the Windows TCP/IP stack incorrectly advances the network buffer by an amount that is 8 bytes too few. This is because the stack internally counts in 16-byte increments, failing to account for the case where a non-RFC compliant length value is used. This mismatch results in the stack interpreting the last 8 bytes of the current option as the start of a second option, ultimately leading to a buffer overflow and potential RCE [2].

Products Affected

Windows 10 (all supported versions), Windows Server 2019, and Windows Server Core (1903, 1909, or 2004) [1, 3].

Recommendations

Install the updates mentioned on Microsoft dedicated page [1].

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

1. **Disable IPv6 if possible**
2. **Disable ICMPv6 RDNSS.**

You can disable ICMPv6 RDNSS, to prevent attackers from exploiting the vulnerability, with the PowerShell command below. This workaround is only available for Windows 1709 and above.

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable
```

The workaround can be disabled with the PowerShell command below.

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=enable
```

> ***Note:*** *No reboot is needed after enabling/disabling the workaround [1].*

In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible.

Detection

Search in all incoming ICMPv6 traffic for packets with an ICMPv6 Type field of 134 – indicating Router Advertisement – and an ICMPv6 Option field of 25 – indicating Recursive DNS Server (RDNSS). If this RDNSS option also has a length field value that is even, the heuristic would drop or flag the associated packet, as it is likely part of a *Bad Neighbor* exploit attempt [2].

A Suricata rule is also available [4].

References

[1] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16898

[2] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-16898-bad-neighbor/

[3] https://blog.rapid7.com/2020/10/14/there-goes-the-neighborhood-dealing-with-cve-2020-16898-a-k-a-bad-neighbor/

[4] https://github.com/advanced-threat-research/CVE-2020-16898