Security Advisory 2023-023

Remote Code Execution vulnerability in Microsoft Message Queuing

April 17, 2023 — v1.0

TLP:CLEAR

History:

- *17/04/2023 — v1.0 – Initial publication*

Summary

On April 11, 2023, Microsoft released a security update for a critical vulnerability in the Microsoft Message Queuing, commonly known as MSMQ [1]. This vulnerability is identified as **CVE-2023-21554** (CVSS score of 9.8) and could allow unauthenticated attackers to remotely execute arbitrary code [2].

Technical Details

The CVE-2023-21554 vulnerability allows an unauthenticated attacker to potentially execute arbitrary code in the context of the Windows service process: `mqsvc.exe`. The attack vector uses the service port `1801/tcp` [3].

Affected Products

MSMQ is provided as **an optional Windows component** and is still available on **all Windows operating systems**, including the latest Windows Server 2022 and Windows 11 [2, 3].

Recommendations

CERT-EU strongly recommends applying the latest patches for Microsoft Windows operating systems. The vulnerability was patched in the April 2023 Security Updates [4].

Mitigations

You can prevent exploitation of this vulnerability by disabling MSMQ, a Windows component that can be turned off through the Control Panel. [2].

In addition, you may block the inbound connections for `1801/tcp` from untrusted sources [3].

Detections

To detect potential exploitation attempts, CERT-EU recommends reviewing network connections on endpoints where the Microsoft Message Queuing service is running (port `1801/tcp`) from unexpected sources, and then, reviewing the potential child processes of `mqsvc.exe` for suspicious events (e.g., `mqsvc.exe` executing `cmd.exe` or `powershell.exe`, among other binaries).

References

[1] https://learn.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472(v=vs.85)

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554

[3] https://research.checkpoint.com/2023/queuejumper-critical-unauthorized-rce-vulnerability-in-msmq-service/?__cf_chl_tk=7J8iZgI93c_ba6v1rOms3UyRgIV9ww0x57IqmNjMQsQ-1681463870-0-gaNycGzNDJA

[4] https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr