MSMQ Remote Code Execution Vulnerability (CVE-2021-25274)

Summary

The Collector Service in SolarWinds Orion Platform versions before 2020.2.4 uses MSMQ (Microsoft Message Queue) and doesn't set permissions on its private queues. As a result, remote unauthenticated clients can send messages to TCP port 1801 that the Collector Service will process. Additionally, upon processing of such messages, the service deserializes them in insecure manner, allowing remote arbitrary code execution as LocalSystem.

Affected Products

- Orion Platform versions 2020.2.1 up to HF 2
- Orion Platform versions 2019.4 up to HF 5
- Orion Platform versions 2019.2 up to HF 3
- Orion Platform versions 2020.2.1 up to HF 2

Fixed Software Release

- Orion Platform 2020.2.4
- Orion Platform 2019.4.2
- Orion Platform 2019.2 HF 4

Acknowledgments

- Martin Rakhmanov, Trustwave

Advisory Details

Severity

8.3 High

Advisory ID

CVE-2021-25274

First Published

02/05/2021

Fixed Version

Orion Platform 2020.2.4, 2019.4.2, 2019.2 HF4

CVSS Score

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H