

# Unprivileged Users can get DBO owner Access Vulnerability (CVE-2021-25275)

## Summary

SolarWinds Orion Platform versions before 2020.2.4, as used by various SolarWinds products, installs and uses a SQL Server back end, and stores database credentials to access this back end in a file readable by unprivileged users. As a result, any user having access to the filesystem can read database login details from that file, including the login name and its associated password. Then, the credentials can be used to get database owner access to the SWNetPerfMon.DB database. This gives access to the data collected by SolarWinds applications, and leads to admin access to the applications by inserting or changing authentication data stored in the Accounts table of the database.

## 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

## 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

8.2 High

#### Advisory ID

[CVE-2021-25275](#)

#### First Published

2/5/2021

#### Fixed Version

Orion Platform 2020.2.4, 2019.4.2, 2019.2 HF4

#### CVSS Score

[CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H](#)