SolarWinds Platform Exposure of Sensitive Information Vulnerability (CVE-2023-23839)

Summary

The SolarWinds Platform was susceptible to the Exposure of Sensitive Information Vulnerability. This vulnerability allows users to access Orion.WebCommunityStrings SWIS schema object and obtain sensitive information.

Affected Products

- SolarWinds Platform 2023.1 and prior versions

Fixed Software Release

- SolarWinds Platform 2023.2

Advisory Details

Severity
6.8 Medium

Advisory ID
CVE-2023-23839

First Published
04/20/2023

Last Updated
04/20/2023

Fixed Version
SolarWinds Platform 2023.2

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

Workarounds

SolarWinds recommends customers upgrade to SolarWinds Platform version 2023.2 as soon as it becomes available. The expected release is by the end of April 2023. SolarWinds also recommends customers to follow the guidance provided in the SolarWinds Secure Configuration Guide. Ensure only authorized users can access the SolarWinds Platform. Special attention should be given to the following points from the documentation:

- Ensure you configure account settings and leverage both account and view limitations, along with module-specific roles only for the tasks they require in their role.