

SolarWinds Platform Incorrect Input Neutralization Vulnerability (CVE-2022-47509)

Summary

The SolarWinds Platform was susceptible to the Incorrect Input Neutralization Vulnerability. This vulnerability allows a remote adversary with a valid SolarWinds Platform account to append URL parameters to inject HTML.

Affected Products

- SolarWinds Platform 2023.1 and earlier

Fixed Software Release

- SolarWinds Platform 2023.2

Acknowledgments

- Juampa Rodriguez (@UnD3sc0n0c1d0)

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:

- Be careful not to expose your SolarWinds Platform website on the public internet. If you must enable outbound internet access from SolarWinds servers, create a strict allow list and block all other traffic. See [SolarWinds Platform Product Features Affected by Internet Access](#).
- Disable unnecessary ports, protocols, and services on your host operating system and on applications like SQL Server. For more details, see the [SolarWinds Port Requirements](#) guide and [Best practices for configuring Windows Defender Firewall](#) (© 2023 Microsoft, available at <https://docs.microsoft.com>, obtained on March 28, 2023.)
- Apply proper segmentation controls on the network where you have deployed the SolarWinds Platform and SQL Server instances.

Advisory Details

Severity

4.3 Medium

Advisory ID

[CVE-2022-47509](#)

First Published

04/18/2023

Last Updated

04/18/2023

Fixed Version

SolarWinds Platform 2023.2

CVSS Score

[CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N](#)