SolarWinds Platform Deserialization of Untrusted Data Vulnerability (CVE-2023-23836)

Security Advisory Summary

SolarWinds Platform version 2022.4.1 was found to be susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to the SolarWinds Web Console to execute arbitrary commands.

Affected Products

- SolarWinds Platform 2022.4.1

Fixed Software Release

- SolarWinds Platform 2023.1

Acknowledgments

- Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative

Workarounds

SolarWinds recommends customers upgrade to SolarWinds Platform version 2023.1 as soon as it becomes available. The expected release is by the end of February 2023. SolarWinds also recommends customers to follow the guidance provided in the SolarWinds Secure Configuration Guide, and 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 January 10, 2023.)

- Apply proper segmentation controls on the network where you have deployed the SolarWinds Platform and SQL Server instances.

- Configure the firewall for the main polling engine to limit and restrict all inbound and outbound access for port 5671. Port 5671 should only communicate to your other SolarWinds Servers (in

---

Advisory Details

Severity

8.8 High

Advisory ID

CVE-2023-23836

First Published

02/15/2023

Last Updated

02/15/2023

Fixed Version

SolarWinds Platform 2023.1

Workarounds

Secure Configuration for the SolarWinds Platform

CVSS Score

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

case of High Availability, both Active and Standby Primary Polling Engine Servers). You can check these by querying the Orion Servers table in the SolarWinds Platform database. Ensure this rule is updated when the configuration of SolarWinds Platform changes, for example, when you add new servers.