SolarWinds Platform Deserialization of Untrusted Data (CVE-2022-38108)

Advisory Details

Severity

7.2 High

Advisory ID

CVE-2022-38108

First Published

10/19/2022

Fixed Version

SolarWinds Platform 2022.4 RC1

CVSS Score

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

Security Advisory Summary

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

Affected Products

- SolarWinds Platform 2022.3 and earlier
- Orion Platform 2020.2.6 HF5 and earlier

Fixed Software Release

- SolarWinds Platform 2022.4 RC1

Acknowledgments

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

Workarounds

SolarWinds recommends customers upgrade to SolarWinds Platform version 2022.4 RC1 as soon as it becomes available. The expected RC release is at the end of October. SolarWinds also recommends that customers 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 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 (© 2021 Microsoft, available at https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring, obtained on January 13, 2021.)
- 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 case of High Availability, both Active and Standby Primary Polling Engine Servers). You can check these by querying the OrionServers 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.