GUIDEPOINT
SECURITY

SOLARWINDS SUPPLY CHAIN ATTACK:
Tactical Information & Recommendations

In order to provide customers with a solid strategy to identify and respond to this attack, as well as to ensure protection against similar types of attacks, GuidePoint Security's DFIR team has developed the following tactical information and recommendations based on details collected from FireEye, Microsoft and SolarWinds reports.

The following information can be used agnostic of any specific toolset while vendors continue to develop product-specific detection capabilities.

Below are the high-level steps that GuidePoint recommends for anyone using SolarWinds Orion, along with supporting technical details.

- **Isolate**
  Ensure that the SolarWinds Orion appliance is isolated from the network until a patch can be deployed. If any evidence of compromise is found it should be further isolated from the internal network.

- **Patch / Stay Up to Date**
  - **SolarWinds:** Organizations leveraging SolarWinds Orion Platform v2020.2 without a hotfix or 2020.2 HF 1 should upgrade ASAP to Orion Platform version 2020.2.1 HF 2 as soon as possible. For more information on SolarWinds' guidance, go to https://www.solarwinds.com/securityadvisory.
  - **Security Products:** As security vendors release additional content related to this attack, it is important to remain up to date and vigilant on what the content detects/protects.

- **Hunt / Validate**
  Multiple Indicators of Compromise (IOCs) have been released thus far in the investigation. Confirm not only whether you were vulnerable, but also leverage the indicators provided here, as well as those distributed by the various vendors, to validate that you haven't been further impacted. GuidePoint recommends that organizations perform threat hunting activities in order to identify if any IOCs are present in their environment.