SolarWinds Security Advisory

Updated: 12.14.2020 12:50pm CST

SolarWinds has just been made aware our systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions **2019.4 HF 5** and **2020.2 with no hotfix** or **2020.2 HF 1**. We have been advised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely targeted, and manually executed attack, as opposed to a broad, system-wide attack. We recommend taking the following steps related to your use of the SolarWinds Orion Platform.

SolarWinds asks customers with any of the below products for **Orion Platform v2020.2 with no hotfix or 2020.2 HF 1** to upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible to ensure the security of your environment. This version is currently available at customerportal.solarwinds.com.

SolarWinds asks customers with any of the below products for **Orion Platform v2019.4 HF 5** to update to **2019.4 HF 6**, which will be available today, December 14, 2020, at customerportal.solarwinds.com.

No other versions of Orion Platform products are known to be impacted by this security vulnerability. Other non-Orion products are also not known to be impacted by this security vulnerability.

If you aren't sure which version of the Orion Platform you are using, see directions on how to check that here. To check which hotfixes you have applied, please go here.

If you cannot upgrade immediately, please follow the guidelines available here for securing your Orion Platform instance. The primary mitigation steps include having your Orion Platform installed behind firewalls, disabling internet access for the Orion Platform, and limiting the ports and connections to only what is necessary.

An additional hotfix release, **2020.2.1 HF 2** is anticipated to be made available Tuesday, December 15, 2020. We recommend that all customers update to release 2020.2.1 HF 2 once it is available, as the 2020.2.1 HF 2 release both replaces the compromised component and provides several additional security enhancements.

Security and trust in our software is the foundation of our commitment to our customers. We strive to implement and maintain appropriate administrative, physical, and technical safeguards, security process, procedures and standards designed to protect our customers.

Known affected products: Orion Platform versions **2019.4 HF 5** and **2020.2 with no hotfix or with 2020.2 HF 1**, including:

Application Centric Monitor (ACM)

Database Performance Analyzer Integration Module (DPAIM)

Enterprise Operations Console (EOC)

High Availability (HA)

IP Address Manager (IPAM)

Log Analyzer (LA)

Network Automation Manager (NAM)

Network Configuration Manager (NCM)

Network Operations Manager (NOM)

Network Performance Monitor (NPM)

NetFlow Traffic Analyzer (NTA)

Server & Application Monitor (SAM)

Server Configuration Monitor (SCM)

Storage Resource Monitor (SCM)

User Device Tracker (UDT)

Virtualization Manager (VMAN)

VoIP & Network Quality Manager (VNQM)

Web Performance Monitor (WPM)

We apologize for any inconvenience caused. For urgent issues, please call Customer Support at 1-866-530-8040 so a support representatives can work on your request. A list of phone numbers can be found on the Contact Us page.