Date: December 21, 2020

Arista Statement Regarding Use of SolarWinds Orion

Arista Networks is providing this security update in response to the cyberattack on the SolarWinds Orion Platform (versions 2019.4 through 2020.2.1 HF10) released between March and June 2020 (Compromised Software).

Arista has not implemented SolarWinds Orion in our development or production environments since 2018. Consequently, Arista has never deployed the Compromised Software in these environments.

From 2018 until December 14, 2020, Arista maintained an instance of SolarWinds Orion in our proof of concept lab environment for customer-led interoperability testing. However, this instance was never upgraded with the Compromised Software. Moreover, this instance was separate from Arista's development, production, and other environments.

As of December 14, 2020, Arista no longer uses SolarWinds Orion in any of its development, testing, production, or other environments.

Based upon the foregoing, we believe that the risk of exposure to the Sunburst/Solarigate attack vector to Arista's systems or products is low. However, we take threats of cyberattacks on our systems and products very seriously and will continue to monitor the situation.

To aid us in this effort, Arista is using the Awake Security Network Detection and Response tool in all of the environments where SolarWinds Orion was deployed with specific detection settings tuned to identify the command and control and malware distribution tools utilized in the Sunburst/Solarigate attack. To date, no markers of a breach have been identified.

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request:

By email: support@arista.com
By telephone: 408-547-5502
866-476-0000