* Our current timeline for this incident begins in September 2019, which is the earliest suspicious activity on our internal systems identified by our forensic teams in the course of their current investigations.
* The subsequent October 2019 version of the Orion Platform release appears to have contained modifications designed to test the perpetrators’ ability to insert code into our builds
* An updated version of the malicious code injection source that inserted the SUNBURST malicious code into Orion Platform releases starting on February 20, 2020.
* The perpetrators remained undetected and removed the SUNBURST malicious code from our environment in June 2020. During that time, through to today, SolarWinds investigated various vulnerabilities in its Orion Platform. It remediated or initiated the process of remediating vulnerabilities, a regular process that continues today. However, until December 2020, the company did not identify any vulnerabilities as what we now know as SUNBURST.
* On December 12, 2020, we were informed of the cyberattack and moved swiftly to notify and protect our customers and to investigate the attack in collaboration law enforcement, intelligence and governments.

As part of our ongoing efforts to protect our customers and investigate the SUNBURST attack, we are reviewing historical and current customer inquiries that might contribute to a better understanding of the attack. To date, we have identified two previous customer support incidents during the timeline referenced above that, with the benefit of hindsight, we believe may be related to SUNBURST. We investigated the first in conjunction with our customer and two third-party security companies. At that time, we did not determine the root cause of the suspicious activity or identify the presence of the SUNBURST malicious code within our Orion Platform software. The second incident occurred in November, and similarly, we did not identify the presence of the SUNBURST malicious code. We are still investigating these incidents and are sharing information related to them with law enforcement to support investigation efforts. We will continue our investigations to help ensure our products and internal systems are secure and to provide information that we hope leads to the identification of the perpetrators and the prevention of these types of attacks in the future. We also plan to continue to share our broader findings with the industry at large in the hope that everyone is better able protect themselves and deliver more secure solutions to their customers.