TS PARTNERS

|630 Freedom Business Center Dr., Suite 212|
|King of Prussia, PA 19406|
|610.768.1100|

December 21, 2020

CVE-2020-10148 SolarWinds ‘Orion’ Supply Chain Attack – TSP Unaffected

Question: 1) Is SolarWinds’ “Orion” used by TSP, or required by Clients in their use of TranStar?

Response: NOT USED

2) Is Microsoft Exchange used by TSP in an internal, on-premise installation?

Response: NOT USED

Background

SolarWinds, FireEye, Microsoft and the CISA have issues alerts that attackers have compromised SolarWinds software development server used to build software updates for the widely-used SolarWinds’ Orion IT network infrastructure management.

The attackers used the compromised build server to insert backdoor malware (called “Sunburst” by FireEye) into the Orion product. **According to SolarWinds, this malware was present as a Trojan Horse in SolarWinds’ Orion Client updates from March through June 2020. Any Orion customer that downloaded the trojaned update also got the malware.**

It has been reported the hackers likely gained access to SolarWinds’ software development environment using an already-compromised (October 2019) Microsoft Office 365 account.

The Sunburst backdoor would allow hackers to further infiltrate other systems at target organizations for reconnaissance/snooping,, data exfiltration, extortion/ransom.

TS Partners and TranStar Unaffected

TS Partners has no relationship with SolarWinds and has never used “Orion”.
TS Partners does not use Microsoft Exchange in on-premise implementation.

Additional Information

https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

For questions regarding Policy, contact CEO or COO

Last Review: December 20, 2021
Last Revision: December 20, 2021