CyberSOC Threat Notification

Vendor: SolarWinds

Published: December 13, 2020

Versions: 2019.4 HF 5 through 2020.2.1

SolarWinds Orion Trojan

Executive Summary

SolarWinds experienced a highly sophisticated, manual supply chain attack on SolarWinds Orion Platform software builds for versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020. The actors behind this attack have trojanized SolarWinds Orion business software and used it to gain access to victim environments. News and information are still very fluid. We are closely monitoring the situation and will send additional bulletins when there are updates.

Description

FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware they named SUNBURST. The campaign is widespread, affecting public and private organizations around the world. Several breaches occurring at government agencies [1] have been attributed to the trojanized version of SolarWinds Orion software. FireEye has released signatures to detect this threat.

Security Risk Advisors is currently scanning CSOC client environments looking for Indicators of Compromise associated with SUNBURST.

Additional Information

- [1] https://www.reuters.com/article/us-usa-solarwinds-cyber-idUSKBN28N0Y7
- https://www.solarwinds.com/securityadvisory
- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://raw.githubusercontent.com/fireeye/sunburst_countermeasures/main/indicator_release/Indicator_Release_Hashes.csv
- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
- https://cyber.dhs.gov/ed/21-01/

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io