SolarWinds Orion

Software Supply-Chain Compromise

TRT Intelligence Advisory

December 15, 2020

Executive Summary

On 13 December 2020, a software supply-chain compromise was reported to have impacted a highly popular SolarWinds' IT monitoring and infrastructure platform, Orion Platform. The compromise is reported to date back to March 2020, in which software updates were laced with malicious code. Tainted software includes Orion Platform versions 2019.4 HF5 – 2020.2.1. SolarWinds has released a patched version, 2020.2.2 HF1 on their customer portal. This supply-chain compromise is being attributed to recently reported high-profile compromises including FireEye and several US government agencies; however, it is likely many other organizations in multiple countries that are customers of SolarWinds may have been compromised.

It is urgently recommended by Fidelis TRT for any customers and users of SolarWinds Orion software to update and install the latest fixes and versions of SolarWinds' Orion software. US CISA has further recommended to federal civilian agencies to disconnect and power down SolarWinds Orion products immediately.

Threat and Technical Data

On 13 December 2020, a software supply-chain compromise was reported to have impacted a highly popular SolarWinds' IT monitoring and infrastructure platform, Orion. The announcement comes approximately one week after cybersecurity and incident response vendor, FireEye/Mandiant, reported a suspected compromise and breach of internally-developed penetration testing and red-teaming tools. The compromise was reported to be attributed to an adversary with state-level support and capabilities.

Further investigation and cooperation with US government agencies, law enforcement, and private sector security companies yielded that the initial point of intrusion and compromise was a tainted software update of SolarWinds' IT management platform, Orion Platform. The campaign was a software supply-chain compromise, in which the source code and valid software was tainted with malicious code and pushed as a legitimate and signed software.

The compromised software update is reported to have been delivered to customers and users of SolarWinds Orion Platform between March – June 2020. Compromised software versions include Orion 2019.4 HF5 – 2020.2.1. SolarWinds released a security advisory in which they stated a patched version, 2020.2.2 HF1, was pushed and available to download from their customer platform.

The malware associated with the infected updates have been dubbed Sunburst/Solerigate. This supply-chain compromise is also being attributed to high-profile attacks recently reported, including the US Treasury, US Chamber of Commerce, US National Telecommunications and Information Administration (NTIA), and FireEye; however, it possible many other organization across multiple countries and verticals may have been impacted.

Conclusion & Assessment

It is urgently recommended by Fidelis TRT for any customers and users of SolarWinds Orion software to install and update to the latest fix for Orion Platform, as prescribed in SolarWinds' security advisory. US CISA has further recommended to federal civilian agencies to disconnect and power down SolarWinds Orion products immediately.

TRT is taking immediate steps to allow detection of instances of the malicious software, including updating our IOC feeds with indicators as well as exploring behavior rules and signatures provided released by US CISA and FireEye.

Software supply-chain attacks are among the most critical and dangerous courses of action that can be carried out by highly complex and well-resourced adversaries. Similar attacks in the recent past include software update compromises of CCleaner (2017), M.E. Docs (2017, which resulted in the global NotPetya ransomware campaign), and Asus computers (2019).

Appendix

Indicators

Please refer *TRT.Service.Bulletin__Sunburst_Solarwinds_Update.Dec_2020* for signatures and indicators being curated and pushed by Fidelis TRT

References:

https://www.solarwinds.com/securityadvisory

https://cyber.dhs.gov/ed/21-01/

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html