SolarWinds Orion

KPMG Cyber Response Services Security Advisory

KPMG is actively monitoring the ongoing security advisory and associated response made public by SolarWinds Worldwide, LLC on Sunday, December 13, 2020. SolarWinds announced to customers that they were the victim of a supply chain attack and specific versions of their SolarWinds Orion product were altered and a backdoor was inserted into the product*. A number of security agencies, including the United States Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), have issued security advisories and bulletins that include detailed information that companies can use to help determine if they may be impacted by the SolarWinds breach.

*Source: SolarWinds Worldwide, LLC

What to do first

If you use the SolarWinds Orion platform in your environment, consider the following recommendations:

Determine the version of SolarWinds Orion deployed in your environment

a) If you are using an impacted version of SolarWinds Orion, please consider the recommendations outlined below in the section titled "I may be impacted, what should I do next?"

b) If you are not using a version of SolarWinds Orion listed on the right, please consider following the recommendations outlined below in the section titled "I may not be impacted, but I want to be cautious."

SolarWinds Orion versions affected

Version	Release Date
2019.4 (Hotfix 5)	March 26, 2020
2020.2	June 4, 2020
2020.2 (Hotfix 1)	June 24, 2020
2020.2.1	August 25, 2020
2020.2.1 (Hotfix 1)	October 29, 2020

I may be impacted, what should I do next?

1. Consider your SolarWinds Orion platform compromised and immediately activate your incident response procedures and follow your company's IR Plan

   a) Based on your IR Plan and associated policies, consider engaging inside and outside counsel for legal guidance and privilege

2. Consider activating your on-call agreement and engaging additional cybersecurity professionals to assist with containment and remediation efforts, as well as to assist with the investigative process

3. Consider evidence that may be required to help answer critical questions and plan your incident response and evidence preservation processes accordingly

   a) For servers impacted by the malicious SolarWinds Orion update packages it may be necessary to acquire an image of physical memory before the server is disconnected from the network or powered down

   b) For servers impacted by the malicious SolarWinds Orion update packages it may also be necessary to capture a full forensic image of the server's file system to support the investigative process

4. Only after you have considered evidence preservation, all SolarWinds Orion servers – including high-availability servers – should be disconnected from the network or otherwise isolated until all servers have been checked and remediated

5. As part of the incident response process, a full investigation should be conducted to better understand the impact to the environment and the company, as well as to support the remediation and restoration processes

   a) There is no "easy check" to determine if your environment has been breached or not

6. Ensure all enterprise security products and monitoring solutions are up-to-date and include detections for the SolarWinds TTPs and IOCs, including third-party security solutions and partners (i.e. MSP, MSSP, etc.)

7. Consider hardening your SolarWinds Orion platform by following the recommendations outlined by SolarWinds in their publication, titled "Secure Configuration for the Orion Platform."

8. Consider revising current and future SolarWinds upgrade plans to address the compromised versions of the platform

   a) Change control processes should be expedited to address the need to test and roll out newer versions of SolarWinds Orion to help mitigate risk and address security concerns

> "The Cybersecurity and Infrastructure Security Agency (CISA) tonight issued **Emergency Directive 21-01**, in response to a known compromise involving SolarWinds Orion products that are currently being exploited by malicious actors. This Emergency Directive calls on all federal civilian agencies to review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately. "

* Source: Cybersecurity and Infrastructure Security Agency

I may not be impacted, but I want to be cautious

1. Incident response professionals (i.e. CIRT team, InfoSec team, etc.) should consult relevant security advisories and bulletins for attacker tactics, techniques and procedures (TTP) as well as indicators of compromise (IOC) and

   a) Check historical log sources using reliable IOCs for evidence of compromise, including EDR, firewall, and DNS log sources

   b) Consider expanding log aggregation and preservation for a period of time to ensure that relevant information is available should SolarWinds expand the number of impacted versions of their Orion platform

2. Implement additional security controls to help identify known IOCs, such as SIEM alerts for notable IP addresses and domain names as well as EDR alerts for notable hash values associated with attacker tools.

3. Consider isolating SolarWinds Orion servers to avoid follow-up attacks now that attacker TTPs have been made public

4. Ensure all enterprise security products and monitoring solutions are up-to-date and include detections for the attack, including third-party security solutions and partners (i.e. MSP, MSSP, etc.)

5. Consider an audit of service and user accounts associated with the SolarWinds Orion platform with an emphasis on new or altered accounts since early 2020 when the supply chain attack was believed to have occurred

Known affected SolarWinds products

Application Centric Monitor (ACM)	Network Automation Manager (NAM)	Server Configuration Monitor (SCM)
Database Performance Analyzer Integration Module (DPAIM)	Network Configuration Manager (NCM)	Storage Resource Monitor (SCM)
Enterprise Operations Console (EOC)	Network Operations Manager (NOM)	User Device Tracker (UDT)
High Availability (HA)	Network Performance Monitor (NPM)	Virtualization Manager (VMAN)
IP Address Manager (IPAM)	Network Traffic Analyzer (NTA)	VoIP & Network Quality Manager (VNQM)
Log Analyzer (LA)	Server & Application Monitor (SAM)	Web Performance Monitor (WPM)

Indicators of compromise (IOC)
Malicious library versions

IOC	Type	SHA256 Hash
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
SolarWinds.Orion.Core.BusinessLayer.dll	Contains Sunburst Backdoor	d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af
app_web_logoimagehandler.ashx.b6031896.dll	Supernova Webshell	c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
C:\WINDOWS\SysWOW64\netsetupsvc.dll	Teardrop Dropper	

Other indicators

IOC	Type	SHA256 Hash
CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp	Sunburst Installer	d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
SolarWinds Worldwide, LLC	SolarWinds Code-signing Certificate	53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7
OrionImprovementBusinessLayer.2.cs	Decompiled Sunburst Source Code	292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712
gracious_truth.jpg	Teardrop Dropper	

Malicious IP addresses & domain names

IOC	Type
*.avsvmcloud[.]com	Domain
deftsecurity[.]com	Domain
freescanonline[.]com	Domain
thedoccloud[.]com	Domain
websitetheme[.]com	Domain
highdatabase[.]com	Domain
incomeupdate[.]com	Domain
databasegalore[.]com	Domain
panhardware[.]com	Domain
zupertech[.]com	Domain
5.252.177.21	IP Address
5.252.177.25	IP Address
13.59.205.66	IP Address
13.65.251.83	IP Address
13.84.134.105	IP Address
13.90.103.231	IP Address
13.92.233.22	IP Address
34.203.203.23	IP Address
51.89.125.18	IP Address
52.170.43.150	IP Address
52.171.135.15	IP Address
52.171.141.69	IP Address
54.193.127.66	IP Address
54.215.192.52	IP Address
107.161.23.204	IP Address
139.99.115.204	IP Address
167.114.213.199	IP Address
192.161.187.200	IP Address
204.188.205.176	IP Address
209.141.38.71	IP Address

This incident represents a supply chain attack. This incident does not represent a vulnerability in SolarWinds’ products.

For more information please contact the below:

Alvin Gan
Executive Director
KPMG in Malaysia
E : alvingan@kpmg.com.my
T : +603 7721 3388

Qadiri, Ubaid Mustafa
Executive Director
KPMG in Malaysia
E : ubaidqadiri@kpmg.com.my
T : +603 7721 3388

Jaco Benadie
Executive Director
KPMG in Malaysia
E : jacobenadie@kpmg.com.my
T : +601 7645 2831

www.kpmg.com.my/CyberResponse

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.