Grant Thornton

The SolarWinds Orion Breach

A supply chain attack on the SolarWinds Orion Platform was made public on December 8, 2020. Several U.S. governmental agencies and other global entities were affected by this highly sophisticated attack.

What is SolarWinds?

SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure.

What is the SolarWinds Orion Breach?

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of active exploitation of SolarWinds Orion Platform software versions 2019.4 HF 5 through 2020.2.1 HF 1, released between March 2020 and June 2020 using a vulnerability, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.

The following are known details about the breach:

- It is a "supply chain breach" – a supply chain breach is one where an attacker compromises some element of software prior to it arriving at the target client environment.
- It has been attributed to an advanced Nation State actor different elements of the U.S. government, technology companies, and of the media. The campaign is widespread, affecting public and private organizations around the world using SolarWinds Orion products.
- The attack leverages multiple techniques to evade detection and obscure their activity.
- The exploit allows the attacker to have the ability to transfer files, execute files, profile the system, reboot the compromised machine, and disable system services.

How did hackers exploit SolarWinds to breach multiple agencies and companies?

The following details have been confirmed by the CISA about the breach:

- The attacker(s) were able to gain access to the software development and production environment within SolarWinds.
- The attacker(s) planted malicious code that got packaged into a digitally signed software update for the SolarWinds Orion product.
- SolarWinds software at client environments downloaded and installed the software update. After the update, the malware activated and allowed attackers to gain access to technology passwords in order to maintain persistence so that they could conduct a variety of other actions (monitor communications, steal data, etc.).
- The tactics, techniques, and procedures that were leveraged by the attackers were intended to blend in with normal client technology operations.
- SolarWinds estimates that approximately 18,000 of its customers have been exposed to the vulnerable product.

Has the vulnerable software been fixed?

SolarWinds has removed the software builds known to be affected from its download sites. They have also released latest hotfixes (emergency patch) to remove any of the malicious code/vulnerabilities identified.

What should a company using SolarWinds Orion running the compromised builds do?

SolarWinds asks customers with any of the below products for Orion Platform version 2020.2 with no hotfix installed, or version 2020.2 HF 1 to upgrade to Orion Platform version 2020.2.1 HF 2 as soon as possible to better ensure the security of your environment. This version is currently available in the SolarWinds Customer Portal[4] at:

- https://customerportal.solarwinds.com

It is also recommended to update the software to release version 2020.2.1 HF 2 as it both replaces the compromised component and provides several additional security enhancements.

How do I confirm if my organization has been breached?

If your organization is not running the known compromised version(s) of SolarWinds Orion (2019.4 HF 5 through 2020.2.1 HF 1), then you could be at lower risk of compromise, but it is still recommended to upgrade to the 2020.2.1 HF 2 version with the latest security patches. It is also recommended to continue to monitor your environment for any malicious or suspicious network activity and follow the Security Advisory page[2] on SolarWinds website, as they update it with the latest information. Additionally, watch out for any bulletins from CISA[1] (https://us-cert.cisa.gov/).

As an added precaution, you may perform a deep-dive activity review on any accounts which have access to your company's most sensitive and confidential data (business secrets, customer data, employee personal data, etc.) and determine if any data was compromised or exfiltrated in the past 6—9 months, or since March 2020.

Merely running the known compromised versions of the SolarWinds Orion (2019.4 HF 5 through 2020.2.1 HF 1) does not mean your organization was compromised. It means that you could have been targeted and/or exploited by the hacker(s)/attacker(s). It is recommended to work with your technical teams (e.g., cybersecurity, networking, information technology teams) and vendor partners to understand if your environment was, or is currently compromised.

Key questions to consider

For CAOs

- What is this SolarWinds breach, and how may it impact our organization?
- Have we thoroughly tested our cyber incident response process, and do recent internal audit findings provide insight into potential issues with our incident response program?
- Do we have confidence in our ability to identify cyber threats within our environment?

For CROs and CCOs

- Do we leverage the software in question and if so, are we responding to contain the event?
- Will this event, or the subsequent remediation, disrupt our business operations?
- Do we need to brief the Board and if so, what do we tell them?
- Do we know if any data was leaked that would cause us to report this event to our customers or regulators?

How Grant Thornton can help

We provide a full suite of cybersecurity and privacy solutions to our clients. Our experience and knowledge of cybersecurity and privacy trends is deep-rooted in our day-to-day interaction with various technology vendors and our diverse portfolio of clients. Our team is capable of providing end-to-end support to our clients for all their cybersecurity needs. Below are some of the most relevant services we provide to our clients facing challenges with cybersecurity and information security:

- **Compromise assessments** – We help evaluate a client environment for the presence of attacker activity leveraging the technical skills of our qualified professionals and our alliance with leading security technology companies like CrowdStrike. Our compromise assessments can assist organizations in understanding if they have been compromised by the SolarWinds attack.
- **Incident Response (IR) services** – We provide comprehensive cyber incident response support to assist clients with detection, containment, and remediation from cyber events such as the SolarWinds attack.
- **Incident Response exercises** – We assist our clients in conducting scenario–based readiness assessments for cyber events to improve the organization's ability to respond to cyber incidents. Exercises can be conducted both at the executive and operations level.
- **Managed Security Services** – We provide 24x7 cybersecurity event monitoring to assist clients with detecting evolving external and internal cyber threats within your environment.

References

1. Cybersecurity and Infrastructure Security Agency (CISA): https://us-cert.cisa.gov/
2. SolarWinds Security Advisory: https://www.solarwinds.com/securityadvisory
3. SolarWinds Security Advisory FAQ: https://www.solarwinds.com/securityadvisory/faq
4. SolarWinds Customer Portal: https://customerportal.solarwinds.com

Grant Thornton