Strategic Perspectives

Wolters Kluwer

December 29, 2020

The Compromise of SolarWinds Orion

By Jena M. Valdetero, and David A. Zetoony, Co-Chairs, U.S. Data, Privacy, and Cybersecurity
Greenberg Traurig, LLP

Amid the holidays and the barrage of pandemic-related news, it has been easy to overlook the reports of a massive security incident that could potentially affect thousands of companies' data. Beginning the week of December 7th, several prominent data breaches were reported by companies and government agencies, including the Department of Homeland Security.

The incidents are linked to a software and network monitoring company based in Austin, Texas called SolarWinds. On its website, SolarWinds claimed to have 300,000 customers, including almost every Fortune 500 company and numerous high-profile federal agencies. One of its products is a network monitoring application called "Orion." The reported breaches were later linked back to a security vulnerability that was introduced by hackers through the Orion platform via a security update in March 2020. The vulnerability is believed to have made at least 18,000 companies vulnerable to data breaches over the past year through the installation of a "back door" which would allow the threat actor access to the environment. SolarWinds introduced a hotfix on December 16, 2020 that they claim will close the backdoor.

What should companies using SolarWinds Orion do?

1. **Investigate a potential breach in accordance with your organization's incident response plan.** The first step is to determine the SolarWinds Orion Platform software build you have installed. The impacted platform versions are 2019.4 HF 5, 2020.2 unpatched, and 2020.2 HF 1. SolarWinds believes that platform version 2019.4 HF 4 (or prior or equal versions) were not compromised. If you are using an impacted platform version, you should assess the products used. SolarWinds claims only certain products are impacted by this security vulnerability. See https://www.solarwinds.com/securityadvisory/faq. If you are not using an impacted platform that does not necessarily mean that you are out of the woods. Some security firms claim to have found malicious code in other SolarWinds products or platform versions. You should continue to monitor the situation to see if those reports are confirmed and if the malicious code is identified as posing a similar security risk.

2. **Disconnect affected SolarWinds servers from your network.** Cutting off any ongoing threat will be key. Be careful, however, not to destroy forensic evidence in the process. As an example, many forensic investigators advise that the server should not be powered off. Preserving evidence, including memory and log files, will be crucial to your investigation.

3. **Retain an external forensic investigation firm**. The best and possibly only way to assess the extent of the compromise and determine what confidential or personal information may have been accessed is to retain a forensic investigator. Given the length of time that your systems may have been vulnerable to this exploit, it is likely that you will lack evidence to conclusively rule out access. However, a forensic investigator can provide useful insight, including whether there are indicators of compromise present that would suggest intrusion by a threat actor.

4. **Retain outside breach legal counsel.** Any third-party forensic investigators should be retained through outside breach counsel to try to maintain attorney-client privilege and work product protections over the underlying investigatory documents which may reveal other security issues unrelated to the SolarWinds attack. It is important to recognize that the underlying *facts* will not be privileged, but the communications and analysis will be to the extent they relate to provision of legal advice. Experienced breach counsel also will be able to assess legal requirements that may flow from unlawful access.

5. **Make a claim with your cyber insurance carrier**. If you have cyber coverage, then the investigatory costs (e.g., forensic investigator, legal counsel, etc.) may be covered under your policy. Note that if the threat actor is determined to be a nation-state actor, it is possible that the claim will ultimately be excluded from coverage by some insurers.

6. **Document your investigation**. As you investigate, your legal counsel should carefully document all steps taken to investigate. A detailed history may be important later to support the reasonableness of your investigation.

7. **Review your obligations to customers or partners.** If your business holds sensitive personal information of individuals with whom you have relationships, and you determine that data may have been accessed, you may have legal obligations under various data breach notification laws to notify individuals. If your business is a third party vendor, you may have both statutory and contractual obligations to notify your business partners.

8. **Review government reporting obligations**. If your company is in a regulated industry (e.g., financial institution, healthcare), you may have obligations to notify a regulatory authority. Government agencies are increasingly issuing requests to registered companies to respond with their plan for addressing the SolarWinds Orion breach. In certain instances, like if you are regulated by the New York Department of Financial Services (NYDFS), state insurance oversight agencies, or the European General Data Protection Regulation (GDPR), the notification obligation may be in a tight timeframe (e.g., 72 hours). Publicly traded companies have obligations to report to the Securities and Exchange Commission (SEC) if a compromise constitutes a material event.

9. **Evaluate contractual indemnification requirements**. To the extent that you may have indemnification obligations to your partners, those should be evaluated and considered.

10. **Rebuild your SolarWinds environment with new servers and updated applications**.

So, you didn't use SolarWinds Orion. Why should you care?

Even if you do not use one of the affected SolarWinds Orion products, you may not be in the clear. Downstream vendors with access to your data/network may be impacted.

1. **Evaluate your legal obligations**. Certain laws require oversight of vendors' information security practices, e.g., Gramm Leach Bliley Act (GLBA), NYDFS Cybersecurity Regulation, and 201 Code of Massachusetts Regulations 17.00, et seq. All 50 U.S. states have data breach notification laws that impose obligations on the "data owner" to notify the individuals and (potentially) regulators if data in the hands of your vendor or licensee is accessed or acquired. Certain federal laws impose similar obligations, e.g., GLBA, HIPAA.

2. **Send an educational advisory to your vendors.** Ensure that your vendors are aware of the SolarWinds Orion issue, and request that they confirm whether they utilized the impacted platforms and programs.

3. **If your vendors are affected, request information about what they are doing to mitigate risk and investigate whether they were compromised.** Specifically, ask them to confirm whether they have hired a forensic investigator to confirm the extent of the impact.

4. **Confirm whether your vendor utilized vendors who were impacted.** Consider the downstream impact on your vendors if *their* vendors may be impacted.

5. **Require affected vendors to update you as their investigation unfolds.** Given that any investigation may take time and facts about the investigation may change, it will be important to require your affected vendors to provide periodic updates.