Quick Reference Guide

SolarWinds Major Security Cyberattack

Why does this cyberattack seem worse? And other FAQ's

Prepared by CONEXXUS HAN SANTOS ATTORNEYS AT LAW

Conexxus, in conjunction with the law firm Han Santos, offers the following synopsis and FAQs to address the serious security attack involving the SolarWinds Orion/IAM® platform (Orion®). First reported by cyber firm FireEye in December 2020, remediation for this security cyberattack is likely to take years.

To our Conexxus members and to the convenience/fuel industry, we recommend that enterprise security response teams 1) audit any use of the Orion® platform and 2) develop third-party risk management programs to review computer resource vendors of any kind.

Background on the Attack

This major security cyberattack has been called the most widespread cyber attack reported to date. A FireEye report in December 2020 stated that organizations using SolarWinds technology had been infiltrated by criminals believed to be associated with Russian intelligence. This action spurred an immediate FBI investigation that concluded the attack probably first occurred in March 2020. The victims of this attack span the private and public sectors, including government, consulting, technology, telecom, and oil and gas companies in North America, Europe, Asia, and the Middle East.

At the center of the attack swirls SolarWinds, a company that provides IT infrastructure management tools to hundreds of thousands of customers, including government agencies, corporations, and nonprofit organizations.

Here's what happened: Malware was inserted within SolarWinds Orion® platform software. If present and activated, this malware potentially allows an attacker to compromise the server on which the Orion® products run[1]. As a result, the criminals were able to infect the networks of many, if not all, of SolarWinds' customers as they updated their SolarWinds' Orion® software in March 2020. According to security experts, the number of infected organizations is estimated at 18,000, including more than 425 of the Fortune 500.

About the Attack

Q: Why is this cyberattack concerning for Conexxus members and the convenience/fuel industry?

A: Not only is this attack extraordinary in its scope, it is devastating in its impact. The attackers were able to gain covert access for approximately nine months without detection. It will be even longer before security experts are able to determine the extent of the information that has been compromised. So, while the attack may have been stopped, the damage could continue for the foreseeable future. While most press has focused on the national security implications of this attack, the impact of this falls equally hard on the business community.

> **"According to security experts, the number of infected organizations is estimated at 18,000, including more than 425 of the Fortune 500."**

Q: Why is SolarWinds cyberattack called a "supply chain hack"?

A: The attack is related to the supply chain of software, not related to merchandise availability or delivery. In this case, the supply refers to the computing resources used by a business. Each computing service provider inevitably relies on computing resources from other vendors, and those vendors rely on yet other vendors. This is the chain to the computer services supply. Because of these links, any retailer or supplier could have been affected by any approved third-party accessing its computers and systems.

Q: What specific software is involved?

A: The attack originated in a routine software update in March 2020 to a SolarWinds product called "Orion Platform, versions 2019.4 HF 5 and 2020.2 with no hotfix installed, or with 2020.2 HF 1." As of now, that update is the only known vector for introducing the malware into other businesses' computers and systems.

[1] SolarWinds Security Advisory, www.solarwinds.com/securityadvisory, December 31, 2020

Quick Reference Guide

Q: What are the impacts of the attack?

A: Even if a company does not directly use Orion®, it could have been infected via connection with another infected computer or system. The malware gives cyber criminals the ability to access, monitor, and control a compromised system, allowing them to destroy or alter data, as well as to impersonate legitimate people like us.

Q: Are there specific recommendations from experts?

A: Yes! General precautions include, but are not limited to, rotating credentials periodically and instituting least privilege protocols. If you are using the Orion® platform, run it in an isolated, secure, standalone account in a cloud services environment. While this is not a perfect isolation, it is better than running it in a combined account where malware could easily have access to sensitive data. Also, change all credentials you control immediately.

Q: What about organizational policy decisions?

A: One strong recommendation is to create a third-party risk management (TPRM) program that covers computer resource vendor access of any kind[2].

About the Cyberattack

Q: Why does this cyberattack seem worse than others?

A: Cloud-integrated IT systems are now ubiquitous. These systems frequently connect to each other via service accounts, API integrations, OAuth tokens, etc., and these connections are cloud-to-cloud, not mediated by any internal networks. This means that many of the tools security teams may be using to monitor their clouds (e.g., Cloud Access Security Brokers "CASBs") will not have visibility into activity[3]. Additionally, Orion® does not display all stored credentials, so IT teams may overlook required credential changes.

Q: What is the nature of the attack?

A: Most known vulnerabilities have been linked to the compromising of API Keys, which require frequent rotation to remain secure. In any security situation, secret data that remains static becomes more vulnerable over time. In the case of Orion®, the compromising of API Keys may give root access to cloud service accounts (e.g., AWS, Azure).

Q: Does this cyberattack indicate that using APIs is unsafe for my business?

A: The short answer is no. APIs are like any other computer interaction that relies on shared secrets, and such interactions are nearly omni-present in today's IT landscape. Key rotation and the use of least privilege architecture designs are proven, strong mitigations.

Q: Do we know anything about retail payment systems being affected?

A: We checked in with Visa and Mastercard, and they let us know that they have run checks on their respective networks without finding any evidence of the malware.

Q: Is Conexxus aware of any issues in its own systems?

A: Conexxus engages in regular and constant review of our vendor software through our internal TPRM. As of now, it looks as though our systems are secure. We do not have any direct use of Orion®, nor do we know of any hidden connections where such software might be used.

Q: What is being done nationally?

A: The Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the Director of National Intelligence (ODNI), along with NSA, have created a task force known as the Cyber Unified Coordination Group (CUCG). This group is charged with coordinating the US government's investigation and remediation of the SolarWinds cyber incident.

The Main Takeaway

Any part of a cloud environment that uses Orion® IAM (Identity and Access Management) must also be considered a threat, because compromised IAM identities could allow attackers access to sensitive resources (e.g., S3 buckets, KMS, Secrets Manager, Lambda) or roles, even ones that are subjected to trust policies[4].

The SolarWinds attack is likely to continue to be an active issue for some time to come. While there is a national effort at remediation, Orion® continues to be a threat. Take appropriate steps to manage any risk.

Co-written by Conexxus and Han Santos

Join us in the conversation.
Join Conexxus membership
and be a part of the solution.

» CONEXXUS MEMBERSHIP

conexxus.org/join

[2] Security Boulevard, https://securityboulevard.com/2020/12/third-party-risk-management-how-to-get-your-vendors-on-board/

[3] SC Media, https://www.scmagazine.com/home/security-news/cloud-security/solarwinds-hack-poses-risk-to-cloud-services-api-keys-and-iam-identities/

[4] Security Boulevard, https://securityboulevard.com/2020/12/the-solarwinds-supply-chain-hack-what-you-need-to-know/