protiviti®
Face the Future with Confidence

SolarWinds Vulnerability Update – Indicators of Compromise and Recommended Actions

18 December
2020

The news of the cyber attacks being experienced by government agencies and an expanding list of organisations continues to grow and change on almost an hourly basis. This is proving to be potentially one of the most significant cyber breaches in recent times. Following up on our 14 December 2020, Flash Report on the CISA advisory, and in response to numerous questions and inquiries we continue to receive, we are providing further detail and insights in this follow-up Flash Report regarding indicators that an organisation's IT environment has been compromised, along with recommended courses of action.

Understanding What Happened

Earlier this week, it was discovered that SolarWinds, a networking software company, had experienced a cyber attack to its systems that inserted a vulnerability in its Orion® Platform software builds that could potentially allow malicious actors to compromise servers on which Orion products run. The attack, disguised within legitimate software updates, distributed a compromised version of the software that was undetectable to system security scanners. The actor appears to follow excellent operational security and is unlikely to share access to this vulnerability with other threat actors.

Cutting through the Jargon

Cyber security uses the term "supply chain attack" in a relatively loose way. When used to describe the SolarWinds Orion incident, it means that the supplier of the software was compromised. In other incidents, it may mean that the distribution channel used to supply software was compromised. At its most broad application, it can refer to a compromise to software or hardware from design to implementation to delivery to the end user.

While the details on the attack are still being investigated, it is clear this was a highly sophisticated supply chain attack. The attacker was able to get malicious code deployed within the SolarWinds network and signed with the SolarWinds code signing certificate. This led to malicious code being pushed to SolarWinds' clients through automated and manual updates of the Orion software. Once the malicious software was in place, the attacker had a back door into the target networks. Given the nature of the SolarWinds Orion use within the

security stack, compromised accounts were highly privileged. The attacker could then be able to collect and exfiltrate information from the target networks.

Due to the sophistication of the attack, it is believed that government agencies and companies with close government ties were the primary targets of the attack. However, organisations using SolarWinds Orion should take actions to mitigate the existing vulnerability and search for malicious activity on their networks.

Immediate Steps to Take

The Cybersecurity & Infrastructure Security Agency (CISA) and U.S. Department of Homeland Security provided required actions and mitigations in their advisory:

- Reimage system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1, and analyse for new user or service accounts.
- Disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from the network.
- Identify the existence of "SolarWinds.Orion.Core.BusinessLayer.dll" and "C:\WINDOWS\SysWOW64\netsetupsvc.dll".
- Block all traffic to and from hosts where any version of SolarWinds Orion software has been installed.
- Identify and remove threat-actor controlled accounts and persistence mechanisms.
- Reset all credentials used by SolarWinds software and implement a rotation policy for these accounts. Require long and complex passwords.
- Update all Orion products to version 2020.2.1 HF2, which was released on 15/12/2020.

FireEye has a running list of mitigations and signatures for various intrusion detection systems available on their GitHub.

Near-Term Steps to Take

- Consider the existence of a malicious SolarWinds Orion version as a vulnerability, but be aware that attackers may have pivoted to other techniques to perform an

actual attack. Detection of a vulnerable version of SolarWinds Orion is not a detection of exploitation without further indicators.

- If SolarWinds Orion is in use, patch it to current and apply the Hotfix.
    - Follow the vendor's guidance for the most up-to-date instructions for patching Orion.
    - Regularly check security tool vendors for advice on updates. Security vendors are regularly updating their products with indicators of compromise (IOCs) produced from the ongoing analysis of this attack.
    - For organisations with endpoint detection and response (EDR) tools, updated scanning and alerting can be found with the vendor, but may also be created from information found in blogs and articles from technical security providers.
    - Alert the managed detection and response (MDR) service provider that the organisation uses SolarWinds Orion and request increased vigilance for related attacks.
- Assess whether other systems may have been impacted. Scan for IOCs and network communication with publicised command-and-control channels. (See "Technical Indicators of Compromise" section below.)
- In the absence of direct indications of compromise, it is difficult to rationally plan a strategy. The SolarWinds Orion vulnerability is unsettling, but without specific IOCs it does not indicate detailed next steps. Once specific response and investigation strategies can no longer be applied, Protiviti recommends using rational goals and a defined scope to guide next steps.
    - Close the incident and maintain enhanced vigilance for a specific period of time. Continue to use emerging threat intelligence to reassess this incident and add new indicators as needed.
    - Define a scope that is most likely to include affected assets and conduct a threat-hunting exercise within this scope. At the conclusion of the exercise, assess whether the scope was sufficient and be prepared to declare the incident closed with appropriate diligence.

As current threat intelligence continues to evolve regarding the potential impact on organisations, leadership will seek assurance that their organisation is secure from the potential threat, and the best way to do this is to follow the steps provided by the various agencies identified in this document and remain vigilant within your networks.

The National Security Agency published an updated Cybersecurity Advisory on Detecting Abuse of Authentication Mechanisms on 17 December 2020.

Medium-Term Items to Consider

- Consider resolving applicable Common Vulnerabilities and Exposures (CVEs) related to the FireEye penetration testing tools stolen in a recent publicly disclosed compromise. These attack tools may soon come into regular use by both financially motivated and less-sophisticated attackers than those responsible for the SolarWinds compromise.
    - FireEye has published over 300 mitigations on its GitHub site for the threats posed by its compromised tools.
- Confirm patching of vulnerable systems or mitigation via compensating controls of systems affected by the 16 CVEs exploited by the FireEye tools.

Long-Term Strategic Planning

- Identify gaps in detection and response, and develop additional capabilities.
- Reassess the threat landscape and adjust strategy based on results.
- Revise the incident response plan to be workable in a crisis and flexible to deal with unforeseen threats. Practice this plan via tabletop exercises and test with wargames.
- Consider adding cyber threat intelligence and threat modelling capabilities to provide direct access to information during emerging events.

Technical Indicators of Compromise

Here is a list of current IOCs that can be used to search for signs of network compromise. FireEye has a running list of mitigations and signatures available on their GitHub for various intrusion detection systems.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti Can Help

Protiviti can assist companies with preparing for and responding to the evolving threats posed by ransomware and other cyberattacks. Contact Protiviti's Incident Response Team at IR@protiviti.com for technical, crisis management and investigative support.

protiviti®