Solarwinds 2020 Cyber Breach

Benjamin Janssens

Independent Researcher

**Executive Summary**

This report aims to outline the cyber breach Solarwinds experienced on their Orion network in 2020. As a result of this breach, nearly every country on Earth was affected; Orion was used in both government and private industries alike. Orion was the name given to a platform of hundreds of different services packaged together intrinsically by Solarwinds. This service provided front-end and back-end management packages of large projects such as industrial control systems or network management, they also catered to small and medium enterprises. The goal of Orion was to simplify these diverse technologies into a centralised software that allowed efficient management (Solarwinds, N.D).

Source code for the Orion project is believed to be leaked via Github, a code repository site, when one of the developers accidentally changed the privilege of the project from private to public (ABC, 2021). As a result, threat actors obtained source code to the enormous Orion project. This facilitated a stealth operation where threat actors could build zero-day attacks around the source code and implement them for future updates. It is believed a relaxed approach to security policy allowed a password of “Solarwinds123” to be used to protect access to the update intranet server, allowing threat actors to plant malware in future updates undetected, although this has never been proven.[[1]](#endnote-1)(Sadler, 2021)

After the incident was discovered, no individuals came forward to claim responsibility or demand a ransom, this has led experts to suggest this hack was intended for gaining knowledge and footholds to influence markets and politics. This was an unprecedented attack and left authorities and Solarwinds in a hard position to manoeuvre forwards efficiently. This was a scenario that forced Solarwinds to decide one of two options, either terminating their software services or starting from essentially scratch. Solarwinds went with the latter and decided to revoke their code signing certificate as this was breached and allowed lateral movement through the company’s network. Although Solarwinds believe they have changed all affiliated code signing certificates, it is believed that this hack has not been eradicated and because of exponential infection rates it may indefinitely be a part of IT systems globally.

**Introduction**

This report will discuss and highlight outcomes and themes around the Solarwinds breach in 2020. This report aims to define the chronological unfolding of the event and who was involved. The report will cover the topics of cybersecurity and industry security practices. The report was conducted using correlational research with both quantitative and qualitative data.

**Investigations / Methodology**

This report will be conducted using correlational Research which is, a Relationship identification between two or more variables. As per Intellithreat’s research policy. Quantitative and qualitative data will be collected as per Intellithreats research policy. Documentation has been stored appropriately and is accessible to Intellithreat intranet as per company policy.

**Findings**

This Report will outline the cyber breach that effected Software developing company Solarwinds and their Orion Product. On 12 December, 2020, cybersecurity firm FireEye stated that it had detected an alleged Russian cyberattack that had compromised Solarwinds security software used on its Orion network[[2]](#endnote-2)(Royal Australian Air Force, 2021). On the 14th of December 2020, Solarwinds was aware of a security breach and issued a disclosure stating “As a part of the ongoing investigation, we have determined that Orion Platform version 2019.4 unpatched, released in October 2019, is the first version in which we have seen activity from the attacker at this time.”[[3]](#endnote-3)(Solarwinds, 2021)

Solarwinds developed an integrated IT platform named Orion, used for monitoring of infrastructure, it created ease for on-site administrative tasks and software as a service (SaaS) environments [[4]](#endnote-4)(Solarwinds, N.D). This created a scalable software that can cover applications from Industrial control systems (ICS) such as dam wall gates or wind turbines and the Internet of Things(IoT) devices that are attached to systems of that size, down to small and medium enterprises that need cloud services and hypervisors.

Software developers coordinated from various locations to create this service. They engaged the help of website Github to store the code they were developing. This allowed software developers to work on the enormous project with less accessibility restrictions. The Australian Broadcasting Corporation (ABC) and other media outlets, made claims that sources within Solarwinds had revealed software developers working on Orion accidently disabled security privileges around the source code on Github, making it open to the public (ABC, 2021) (Thomas, 2020).[[5]](#endnote-5)[[6]](#endnote-6) This gave threat actors a plethora of information that could be weaponized against Solarwinds, akin to getting the blueprints for a bank robbery. It is believed that on this Github forum, the password of “Solarwinds123” was stored in records and implied it was used around intrinsic network protocols and devices such as routers and switches, and the update server for future Orion and other Solarwinds products distributions[[7]](#endnote-7)(Sadler, 2021)

The Initial malware discovered on the Orion platform was named SUNBURST. Solarwinds described the malware, officially named CVE-2022-36963 (NIST, 2020)[[8]](#endnote-8) saying “The SolarWinds Platform was susceptible to the Command Injection Vulnerability. This vulnerability allows a remote adversary with a valid SolarWinds Platform admin account to execute arbitrary commands.”[[9]](#endnote-9)(Solarwinds, 2023) This meant the threat actors could modify aspects of many different parts of the software with administrative privileges. This poisoned the well and meant it was impossible to tell what parts of code was untouched and what was compromised. This facilitated stealth operations for the threat actors as it was no different to dealing with a zero-day attack.

As software gets distributed by companies, more often than not, quality of use feedback gets developed overtime, updates and features can be added and improve the software. Like when using Microsoft Office, you must enter a licensing key to use the software. This key is generated from an algorithm but is not individually assigned by the company. This means that it is possible to guess the license key to a software, like guessing someone’s bankcard numbers. Solarwinds stated “SolarWinds uses a digital code-signing certificate to digitally sign each software build, and to help end users authenticate the code comes from us.”[[10]](#endnote-10)(Solarwinds, 2021)

Solarwinds stated “As part of our response to the SUNBURST vulnerability, the code-signing certificate used by SolarWinds to sign the affected software versions was revoked March 8, 2021. This is industry-standard best practice for software that has been compromised. Regretfully, the same digital code-signing certificate used to sign our Orion Platform software affected by the SUNBURST vulnerability was also used to sign additional SolarWinds products not known to be affected by SUNBURST. While this does not mean all products are compromised, it does mean the day-to-day operation of any software signed by the compromised digital code signing certificate may be impacted by a user’s operating system, antivirus, or endpoint protection software after the certificate was publicly revoked on March 8, 2021”[[11]](#endnote-11)(Solarwinds, 2021).

This led to several malwares stemming from SUNBURST to be discovered. The Australian Cyber Security Centre (ACSC) released an official report stating “Following the identification of SUNBURST, additional malware associated with the SolarWinds Orion supply chain compromise has been identified. These are commonly being referred to as TEARDROP and RAINDROP and have been identified during investigations of follow-on compromises of affected organisations. During investigations of the supply chain compromise, additional malware targeting SolarWinds Orion was identified. This second set of malicious software is being referred to as SUPERNOVA. The SUPERNOVA malware is not believed to be related to the supply chain compromise, instead targeting an unrelated vulnerability in SolarWinds Orion”[[12]](#endnote-12)(ACSC, 2021).

Solarwinds realized the scale of the attack and the substantial number of assets effected. Customers of Solarwinds range from the US Pentagon and advanced weapon manufacturers to small businesses in Australia. It has been reported that U.S. Government entities includes the Commerce Department, the Pentagon, the Department of Homeland Security, the U.S. Postal Service, the Treasury Department and the National Institutes of Health [[13]](#endnote-13)(NPR, 2020).

This incident forced the industry to rethink its approach to policy and procedures around security and accessibility. A spotlight was pointed at all corners of this incident and addressed issues such as generic password use for intrinsically based security elements, Company policies regarding the distribution of proprietary intellectual property and access to this data. This case defined the issues surrounding software distribution and who the victims of unregulated software security policy and legislation really are.

**Conclusions**

To conclude this report, the issues surrounding industry security policies must be highlighted. Companies with access to data, intellectual property and the physical mediums that enabled Solarwinds to possess power over huge societal leaders such as government or big stock market companies, needs to be addressed. Specifically the relaxed attitude surrounding security. Transparency and accountability for companies and their staff’s actions should be documented and reviewed in government mandated auditing procedures. Governments need to provide a space with funding to help protect its citizens data. The cohesion of Government and the private sector could make the internet a much safer place for all its users.

**Recommendations**

I recommend that government tighten legislation surrounding data collection, development and privacy, especially around the mediums that allow the data to be accessed. Air gapped facilities and zero trust networks could be implemented around such serious data. This kind of protection is expensive and does not align with companies profit margins, hence, the government needs to mandate this kind of protection.

**Attachments**

**References**

1. <https://ia.acs.org.au/article/2021/the-intern-did-it--solarwinds-ceos-pass-blame.html> (Sadler. DS. 2021: The intern did it: SolarWinds CEOs pass blame: ACS) [↑](#endnote-ref-1)
2. <https://runway.airforce.gov.au/resources/link-article/australia-must-do-more-prepare-solarwinds-style-supply-chain-attack> (Uren. TU. 2021. Australia must do more to prepare for a Solarwinds-style supply-chain attack: RAAF) [↑](#endnote-ref-2)
3. <https://www.solarwinds.com/sa-overview/securityadvisory> (Solarwinds. 2021. Security Advisory: Solar Winds) [↑](#endnote-ref-3)
4. <https://www.solarwinds.com/orion-platform> (Solarwinds. N.D. Orion Platform: Solarwinds) [↑](#endnote-ref-4)
5. <https://www.youtube.com/watch?v=YbxMOXyq5eM> (ABC. 2021. Infamous Solarwinds attack started with two simple mistakes: ABC) [↑](#endnote-ref-5)
6. <https://www.theregister.com/2020/12/16/solarwinds_github_password/> (Thomas. TC. 2020. We're not saying this is how SolarWinds was backdoored, but its FTP password 'leaked on GitHub in plaintext': TheRegister) [↑](#endnote-ref-6)
7. <https://ia.acs.org.au/article/2021/the-intern-did-it--solarwinds-ceos-pass-blame.html> (Sadler. DS. 2021: The intern did it: SolarWinds CEOs pass blame: ACS) [↑](#endnote-ref-7)
8. <https://nvd.nist.gov/vuln/detail/CVE-2022-36963> (NIST. 2020. National Vulnerability Database: NIST) [↑](#endnote-ref-8)
9. <https://www.solarwinds.com/trust-center/security-advisories/cve-2022-36963> (Solarwinds. 2023) [↑](#endnote-ref-9)
10. <https://www.solarwinds.com/sa-overview/new-digital-certificate> (Solarwinds. 2021. SolarWinds New Digital Code-Signing Certificate: Solarwinds) [↑](#endnote-ref-10)
11. <https://www.solarwinds.com/sa-overview/new-digital-certificate> (Solarwinds. 2021) [↑](#endnote-ref-11)
12. <https://www.cyber.gov.au/about-us/alerts/potential-solarwinds-orion-compromise> (ACSC. 2021) [↑](#endnote-ref-12)
13. <https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little> (NPR, 2020) [↑](#endnote-ref-13)