riskrecon

mastercard

The State of the Global Response to the SolarWinds Orion Breach

A view from the Internet that yields important lessons for managing enterprise cybersecurity risks

February 15, 2021

www.riskrecon.com

sales@riskrecon.com

1493 W 200 S

Salt Lake City, UT

(801) 758-0560

Introduction

The SolarWinds Orion breach provides a unique opportunity to understand how organizations respond to a high-profile threat that yield important lessons for managing enterprise cybersecurity risks. How many have shut their Orion systems? How many have upgraded their systems to address the vulnerability? While no one has the visibility into the internals of all organizations to answer these questions, analysis of the Orion systems operating on the Internet provide a window into how the world has responded to the threat.

RiskRecon has monitored the exposure and response to SolarWinds Orion through its Internet-scale opensource security intelligence engines. This paper presents RiskRecon's analysis of the exposure on February 1, 2021, comparing that with exposure on December 13, 2020, the day of the public breach disclosure, and February 1.

Take-Aways for CISO

The SolarWinds Orion breach and the observable response provide a valuable window into how organizations respond to critical threats.

- Good news – Organizations observably acted to reduce their Orion exposure. Across the Internet population, 25% of organizations responded by removing their SolarWinds systems from the Internet. While we can't tell if they permanently shut down Orion or if they properly quarantined them behind a firewall, it is good to see action being taken.
- Good news – There is strong evidence that third-party risk programs were impactful in reducing Orion risk exposure. For companies who are subject to strict third-party risk governance by their customers, over 50% shutdown their Internet-facing Orion instances – over 2x higher than the general population.
- Bad news – If you think other entities can be trusted to protect your risk interests, think again. Most organizations took no action, with 75% leaving their Orion instances exposed to the Internet. Unfortunately, these were not insignificant organizations. They include universities, state and local governments, Fortune 500 companies, and system hosting providers.
- Bad news – Compounding on the negligence many companies demonstrated, of those who left their Orion instance exposed to the Internet, only 8% applied the SolarWinds-required security patches.

Background

On December 13, 2020, the Department of Homeland Security announced that malicious actors were actively exploiting SolarWinds Orion versions 2019.4 through 2020.2.1 HF1. As there was no mitigation, the DHS advised government agencies to disconnect systems operating the affected versions. This sent shockwaves through the industry, as numerous entities such as FireEye, Microsoft, Mimecast, the Department of Commerce, and the Department of Justice disclosed they were breached.

Since the breach, SolarWinds has urged customers to upgrade to Orion 2020.2.4. The SUNBURST attack referred to specific versions of 2019.4 and 2020.2.2 that contained backdoor code that was actively

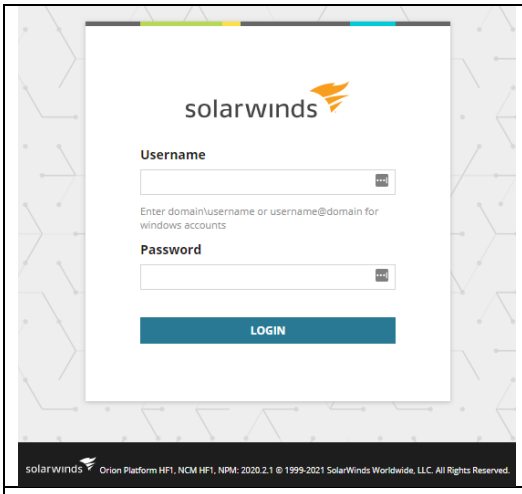
compromised. Another malware, named SUPERNOVA, impacted a wider set of Orion versions. SolarWinds' security advisory is available at https://www.solarwinds.com/securityadvisory.

Upon disclosure of the SolarWinds breach, RiskRecon immediately focused its opensource intelligence analytics engines on helping its customers and the larger community to identify potentially breached companies. Since December 13, 2020 RiskRecon has monitored SolarWinds exposure, providing a valuable view into how companies have responded to the incident.

Methodology

As a global provider of cybersecurity ratings and insights, RiskRecon conducts Internet-wide security assessment of systems and applications. A foundation of RiskRecon's analytics is its global port scanning and web crawling operations and analytics, giving it multiple angles of visibility into the security state of enterprises and their systems.

Leveraging this foundation, on December 13, 2020, and again on February 1, 2021, RiskRecon enumerated all Internet-facing systems operating an Orion web administration interface and the associated version of the Orion software. SolarWinds Orion reveals the presence of its administration interface through HTTP header values. Orion reveals its version in the administration interface HTML. Below are three example screenshots of the Orion administration interfaces. Ironically, the instance on the right prominently displays a SSAE16 certification on an unpatched software platform.



Example interface for Orion 2020.2.1 HF1

Example interface for Orion 2013.2.1

Findings

How Many Companies are Operating Orion on the Internet?

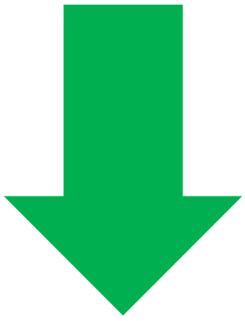
As measured from the Internet, the largest observable response to the SolarWinds Orion threat has been to shut down their SolarWinds systems, or at least pull them from the Internet. In the 50 days since the disclosure of the SolarWinds Orion breach, the number of entities operating any version of Orion directly on the Internet decreased by 25%. On December 13, 2020, RiskRecon observed 1,785 organizations exposing SolarWinds Orion to the Internet, about 5% of all Orion customers. By February 1, 2021, the number of companies doing so decreased to 1,330.

Change in SolarWinds Orion on the Internet
12/13/20 to 2/1/21 - All Companies

25%

The results are much more impressive for companies who have customers that actively monitor the cybersecurity risk of their vendors. Over the same timeframe, vendors of RiskRecon customers that use RiskRecon to monitor vendor security risk decreased their operation of SolarWinds Orion on the Internet by 52%. On December 13, 2020 RiskRecon observed 209 vendors of RiskRecon third-party risk management customers operating Orion on the Internet. By February 1, 2021, the number of companies doing so decreased to 100.

Change in SolarWinds Orion on the Internet
Vendors of RiskRecon Customers
12/13/20 to 2/1/21



52%

The 2x greater decrease of operation of Orion on the Internet by vendors of RiskRecon customers is strong evidence of the value of third-party risk management teams and leveraging data to better manage supply chain risk. In the face of the SolarWinds Orion threat, many third-party risk teams leveraged RiskRecon to identify vendors running Orion and reached out to those companies to ensure they were properly addressing the risks.

Are Companies Patching the Orion Software?

Shortly after disclosing the breach, SolarWinds advised customers to upgrade to Orion 2020.2.4 or Orion 2019.4.2 to address the SUNBURST and SUPERNOVA issues. Based on RiskRecon's analysis, only 8% of

companies that continue to operate SolarWinds on the Internet have followed the security advisory and upgraded to a required version.

Percent of Companies that Applied Security Fix

As visible to RiskRecon from the Internet

8%

Given that Orion SUNBURST and SUPERNOVA are such highly visible security issues, it is disappointing to see such a small number of instances being patched. Of all Orion systems, these systems exposed directly to the Internet are arguably the most vulnerable, with less compensating controls to mitigate risks.

Of the companies operating SolarWinds Orion directly on the Internet, 4% are operating a version that contains the SUNBURST malicious code. While the SUNBURST command and control channel has been disabled, these organizations are still exposed to SUPERNOVA. In total, 37% are operating a version that is vulnerable to the SUPERNOVA exploit.

Percent of Companies Operating SUNBURST Version

4%

Percent of Companies Operating SUPERNOVA Vulnerable Version

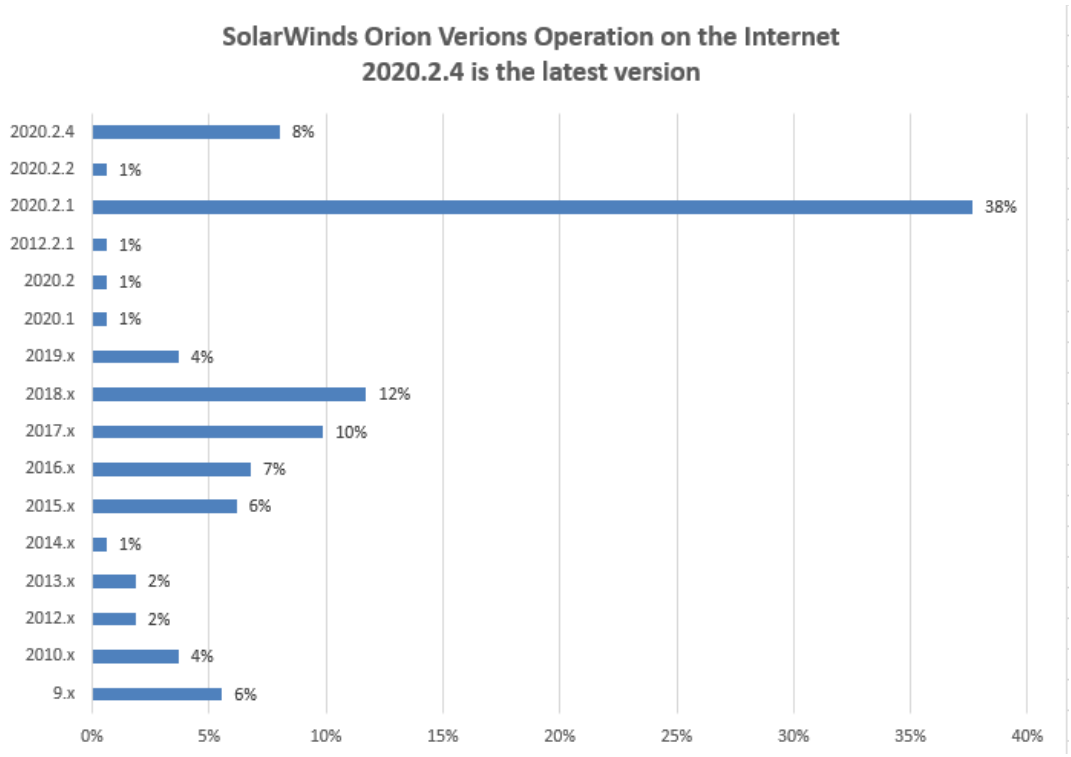
37%

As visible to RiskRecon from the Internet

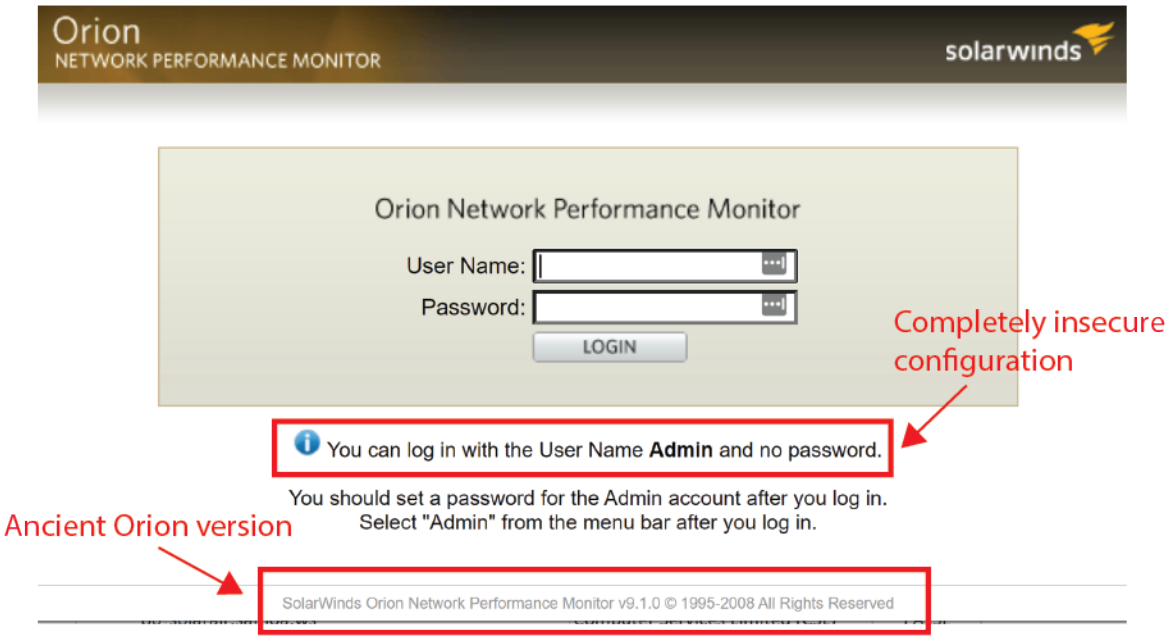
Unfortunately, the organizations running these vulnerable instances on the Internet are not insignificant. They include universities, state and local governments, Fortune 500 companies, and system hosting providers.

Observed Versions of SolarWinds Orion

The most common Orion version observed operating on the Internet was 2020.2.1 HF2, accounting for 31% of the total. Among the population, RiskRecon observed versions as old as version 9.0.0, released circa 2008 – 13 years ago!



The screenshot below is an example of a particularly a particularly ancient instance running SolarWinds Orion 9.1.0, shown at the bottom of the screenshot. Even worse, notice the information tip advising that "You can log in with the User Name Admin and no password."



Conclusion

Organizations are critically dependent on each other to provide systems and services necessary to operate. As organizations interconnect with other entities, they depend on their vendors and partners to protect their risk interests. The SolarWinds Orion breach and the observable response provide a valuable window into how organizations respond to critical threats.

On the positive side, we observed that 25% of organizations responded by pulling their Orion instances from the Internet. Even more positive is that there is very strong evidence that third-party risk management works! Companies who are subject to strong third-party risk management from their customers performed dramatically better than the general population, decreasing their Internet-facing Orion instances by 52%.

On the downside, most companies showed little or no response to the Orion breach. Seventy-five percent of organizations left their Orion administration interfaces exposed to the internet. Of these organizations, only 8% applied the SolarWinds-required security patches.

About RiskRecon

RiskRecon, a Mastercard company, provides cybersecurity ratings and insights that make it easy for organizations to understand and act on their risks. Customers use the RiskRecon platform to better manage their own enterprise, third-party, supply chain, and merger and acquisition risks. RiskRecon is the only cybersecurity rating platform that delivers risk-prioritized action plans custom-tuned to match your risk priorities and appetite. Learn more at https://www.riskrecon.com