UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT

PURSUANT TO SECTION 13 OR 15(d) OF
THE SECURITIES EXCHANGE ACT OF 1934

December 17, 2020
Date of Report (Date of earliest event reported)

SOLARWINDS CORPORATION

(Exact name of registrant as specified in its charter)

Delaware	**001-38711**	**81-0753267**
(State or other jurisdiction of incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

7171 Southwest Parkway
Building 400
Austin, Texas 78735
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code: (512) 682-9300

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	**Trading Symbol**	**Name of Each Exchange on Which Registered**
Common Stock, $0.001 par value	SWI	New York Stock Exchange

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 7.01 Regulation FD Disclosure.

On December 14, 2020, SolarWinds Corporation ("SolarWinds" or the "Company") filed a Current Report on Form 8-K disclosing that it had been made aware of a potential security incident with respect to its Orion monitoring products. On December 17, 2020, SolarWinds provided the following update on the security incident on its Orange Matter corporate blog, accessible at: https://orangematter.solarwinds.com:

On Saturday, December 12, our CEO was advised by an executive at FireEye of a security vulnerability in our Orion Software Platform which was the result of a very sophisticated cyberattack on SolarWinds. We soon discovered that we had been the victim of a malicious cyberattack that impacted our Orion Platform products as well as our internal systems. While security professionals and other experts have attributed the attack to an outside nation-state, we have not independently verified the identity of the attacker.

Immediately after this call, we mobilized our incident response team and quickly shifted significant internal resources to investigate and remediate the vulnerability. Know that each of our 3,200 team members is united in our efforts to meet this challenge. We remain focused on addressing the needs of our customers, our partners and the broader technology industry.

To accomplish that, we swiftly released hotfix updates to impacted customers that we believe will close the code vulnerability when implemented. These updates were made available to all customers we believe to have been impacted, regardless of their current maintenance status. We have reached out and spoken to thousands of customers and partners in the past few days, and we will continue to be in constant communication with our customers and partners to provide timely information, answer questions and assist with upgrades.

We are solely focused on our customers and the industry we serve. Our top priority has been to take all steps necessary to ensure that our and our customers' environments are secure. We are taking extraordinary measures to accomplish this goal. We shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed to do their research. We also have had numerous conversations with security professionals to further assist them in their research. We were very pleased and proud to hear that colleagues in the industry discovered a "killswitch" that will prevent the malicious code from being used to create a compromise.

Here are a few important things to know:

- This was a highly sophisticated cyberattack on our systems that inserted a vulnerability within our Orion® Platform products. This particular intrusion is so targeted and complex that experts are referring to it as the SUNBURST attack. The vulnerability has only been identified in updates to the Orion Platform products delivered between March and June 2020, but our investigations are still ongoing. Also, while we are still investigating our non-Orion products, to date we have not seen evidence that they are impacted by SUNBURST.

- The vulnerability was not evident in the Orion Platform products' source code but appears to have been inserted during the Orion software build process.

- We swiftly released hotfix updates to impacted customers, regardless of their maintenance status, that we believe will close the vulnerability when implemented.

- After our release of Orion 2020.2.1 HF2 on Tuesday night, we believe the Orion Platform now meets the US Federal and state agencies' requirements. We are providing direct support to these customers and will help them complete their upgrades quickly.

- We are continuing to take measures to ensure our internal systems are secure, including deploying the Falcon Endpoint Protection Platform across the endpoints on our systems.

- We have retained industry-leading third-party cybersecurity experts to assist us with this work and are actively collaborating with our partners, vendors, law enforcement and intelligence agencies around the world.

We are providing our customers, experts and others in the IT and security industries detailed information regarding the incident to aid with identifying indicators of compromise and steps they can take to further harden their systems against unauthorized incursion. These tools can be found on our Security Advisory page at www.solarwinds.com/securityadvisory which we are updating as we learn new information.

Our shared goal is to better understand and protect against these types of malicious attacks in the future.

As we've noted, the attacks on our systems were incredibly complex, and it will take some time for our investigative work to be complete. We are committed to being deliberate as we take this on. At the same time, of course, we know that we are the subject of scrutiny and speculation. In order to be as clear as possible, we want to highlight that the exploration by SolarWinds of the potential spinoff of its MSP business and the departure of our CEO, were announced in August 2020. Finally, all sales of stock by executive officers in November were made under pre-established Rule 10b5-1 selling plans and not discretionary sales.

We understand and share our customers' and the industry's concerns, and we are grateful for the continued support and understanding that we have received. We will continue to investigate these matters and share what information we can to continually find ways to improve our collective security from these types of attacks.

Forward-Looking Statements

This communication contains "forward-looking" statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, including statements regarding SolarWinds' understanding of the vulnerability that was inserted within its Orion monitoring products, the potential sources of these security incidents, SolarWinds' response to the security incidents and related investigations, the status of and facts uncovered in its investigations to date, SolarWinds' efforts to improve the security of its products and its customers and its environments. These forward-looking statements are based on management's beliefs and assumptions and on information currently available to management, which may change as the investigations proceed and new or different information is discovered. Forward-looking statements include all statements that are not historical facts and may be identified by terms such as "aim," "anticipate," "believe," "can," "could," "seek," "should," "feel," "expect," "will," "would," "plan," "intend," "estimate," "continue," "may," or similar expressions and the negatives of those terms. Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by the forward-looking statements. Our investigations are still at their early stages and are on-going, including the work required to understand the root cause analysis of the attack and to ensure that our and our customers' environments are secure and to fully assess and, if required, remediate any vulnerabilities within the Orion Platform products and to assess whether other vulnerabilities exist with the Orion Platform products or in SolarWinds' other products and services. Factors that could cause or contribute to actual results, performance or achievements to be different include, but are not limited to, (a) the discovery of new or different information regarding the vulnerability within SolarWinds' Orion Platform products or of additional vulnerabilities within, or attacks on, the Orion Platform products or any of SolarWinds' other products, services and systems, (b) the discovery of new or different information regarding the exploitation of the vulnerability in the Orion Platform products, (c) the possibility that SolarWinds' mitigation and remediation efforts with respect to its Orion Platform products and/or internal systems may not be successful, (d) the possibility that customer, personnel or other data was exfiltrated as a result of the vulnerability in the Orion monitoring products, (e) numerous financial, legal, reputational and other risks to SolarWinds related to the security incidents, including risks that the incidents may result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or vendor relationships and investor confidence, U.S. or foreign regulatory investigations and enforcement actions, litigation, indemnity obligations, damages for contractual breach, penalties for violation of applicable laws or regulations, significant costs for remediation and the incurrence of other liabilities, (f) risks that SolarWinds' errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be available or sufficient to compensate for all liabilities SolarWinds incurs related to the incidents and (g) such other risks and uncertainties described more fully in documents filed with or furnished to the U.S. Securities and Exchange Commission by SolarWinds, including the risk factors discussed in SolarWinds' Annual Report on Form 10-K for the period ended December 31, 2019 filed on February 24, 2020, its Quarterly Report on Form 10-Q for the quarter ended March 31, 2020 filed on May 8, 2020, its Quarterly Report on Form 10-Q for the quarter ended June 30, 2020 filed on August 10, 2020 and its Quarterly Report on Form 10-Q for the quarter ended September 30, 2020 filed on November 5, 2020. All information provided in this communication is as of the date hereof and SolarWinds undertakes no duty to update this information except as required by law.

The information contained in this Current Report on Form 8-K pursuant to this "Item 7.01 Regulation FD Disclosure" shall not be deemed "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), or otherwise subject to the liability of that section. The information in this section of this Current Report on Form 8-K shall not be incorporated by reference in any filing under the Securities Act of 1933, as amended, or the Exchange Act except as shall be expressly set forth by specific reference in such a filing.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

SOLARWINDS CORPORATION

Dated: December 17, 2020

By: /s/ Kevin B. Thompson
Kevin B. Thompson
President and Chief Executive Officer