AlphaSense Highlighted Document

SolarWinds Corporation (SWI)

Other Events

14-Dec-20 8K

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 14, 2020
Date of Report (Date of earliest event reported)

SOLARWINDS CORP ORATION

(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.

©2017, AlphaSense, Inc. All Rights Reserved. AlphaSense is a service mark of AlphaSense, Inc. All other trademarks mentioned belong to their respective owners.

©2017, AlphaSense, Inc. All Rights Reserved. AlphaSense is a service mark of AlphaSense, Inc. All other trademarks mentioned belong to their respective owners.

Item 8.01 Other Events.

SolarWinds Corporation (***"SolarWinds" or the "C***ompany") has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. ***SolarWinds*** has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state, but ***SolarWinds*** has not independently verified the identity of the attacker. ***SolarWinds*** has retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans. ***SolarWinds*** is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.

Based on its investigation to date, ***SolarWinds*** has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 (the "Relevant Period"), was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products. ***SolarWinds*** has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken. ***SolarWinds*** is not currently aware that this vulnerability exists in any of its other products.

SolarWinds currently believes that:

- Orion products downloaded, implemented or updated during the Relevant Period contained the vulnerability;
- Orion products downloaded and implemented before the Relevant Period and not updated during the Relevant Period did not contain the vulnerability;
- Orion products downloaded and implemented after the Relevant Period did not contain the vulnerability; and
- Previously affected versions of the Orion products that were updated with a build released after the Relevant Period no longer contained the vulnerability; however, the server on which the affected Orion products ran may have been compromised during the period in which the vulnerability existed.

SolarWinds values the privacy and security of its over 300,000 customers and is working closely with customers of its Orion products to address this incident. On December 13, 2020, ***SolarWinds*** delivered a communication to approximately 33,000 Orion product customers that were active maintenance customers during and after the Relevant Period. ***SolarWinds*** currently believes the actual number of customers that may have had an installation of the Orion products that contained this vulnerability to be fewer than 18,000. The communication to these customers contained mitigation steps, including making available a hotfix update to address this vulnerability in part and additional measures that customers could take to help secure their environments. ***SolarWinds*** is also preparing a second hotfix update to further address the vulnerability, which ***SolarWinds*** currently expects to release on or prior to December 15, 2020. For the nine months ended September 30, 2020, total revenue from the Orion products across all customers, including those who may have had an installation of the Orion products that contained this vulnerability, was approximately $343 million, or approximately 45% of total revenue.

There has been significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products. ***SolarWinds*** is still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks.

SolarWinds uses Microsoft Office 365 for its email and office productivity tools. ***SolarWinds*** was made aware of an attack vector that was used to compromise the Company's emails and may have provided access to other data contained in the Company's office productivity tools. ***SolarWinds,*** in collaboration with Microsoft, has taken remediation steps to address the compromise and is investigating whether further remediation steps are required, over what period of time this compromise existed and whether this compromise is associated with the attack on its Orion software build system. ***SolarWinds*** also is investigating in collaboration with Microsoft as to whether any customer, personnel or other data was exfiltrated as a result of this compromise but has uncovered no evidence at this time of any such exfiltration.

SolarWinds' investigations into these matters are preliminary and on-going, and Sola***rWinds is*** still discerning the implications of these security incidents. During the course of these investigations, ***SolarWinds*** may become aware of new or different information. At this time, ***SolarWinds*** is unable to predict any potential financial, legal or reputational consequences to the Company resulting from this incident, including costs related thereto. So as not to compromise the integrity of any investigations, ***SolarWinds*** is unable to share additional information at this time.

©2017, AlphaSense, Inc. All Rights Reserved. AlphaSense is a service mark of AlphaSense, Inc. All other trademarks mentioned belong to their respective owners.

Forward-Looking Statements

This Current Report on Form 8-K 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 and the attack vector that was used to compromise SolarWinds’ em***ails and may ha***ve provided access to other data contained in the Company's office productivity tools, the potential sources of these security incidents, the number of SolarWinds customers t***hat may ha***ve had an installation of SolarWinds’ Orion prod***ucts that conta***ined the vulnerability and the revenue related thereto, SolarWinds’ response to th***e security inci***dents, the status and results of its investigations to date and the potential impact of these incidents on its business operations and financial results and condition. These forward-looking statements are based on management's beliefs and assumptions and on information currently available to management, which may change as 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. Factors that could cause or contribute to such differences include, but are not limited to, (a) the discovery of new or different information regarding the vulnerability within ***SolarWinds’ Ori***on monitoring products and/or the compromise of Sola***rWinds ema***ils and other office productivity tools or of additional vulnerabilities within, or attacks on, Sola***rWinds’ product***s, services and systems, (b) the discovery of new or different information regarding the exploitation of the vulnerability in the SolarWin***ds’ Orion monit***oring products and/or the compromise of SolarWinds e***mails and*** other office productivity tools, (c) the possibility that SolarWinds’ ***mitigation and*** remediation efforts with respect to its Orion monitoring 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 compromise to SolarWinds’ emai***ls and other of***fice productivity tools, (e) numerous financial, legal, reputational and other risks to SolarWinds related t***o the secu***rity 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 a***nd omissions in***surance coverage covering certain security and privacy damages and claim expenses may not be available or sufficient to compensate for all liabilities SolarWinds incurs relate***d to the i***ncidents 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 th***e risk fact***ors discussed in SolarWinds’ Annual Repor***t 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 Current Report on Form 8-K is as of the date hereof and ***SolarWinds*** undertakes no duty to update this information except as required by law.

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 14, 2020

By: /s/ Kevin B. Thompson

Kevin B. Thompson

President and Chief Executive Officer

©2017, AlphaSense, Inc. All Rights Reserved. AlphaSense is a service mark of AlphaSense, Inc. All other trademarks mentioned belong to their respective owners.