SolarWinds CEO apologizes for blaming an intern, says attack may have started in January 2019

therecord.media/solarwinds-ceo-apologizes-for-blaming-an-intern-says-attack-may-have-started-in-january-2019/

May 19, 2021

Corporate keynotes at the annual RSA Conference are generally uneventful PR opportunities for executives and vendors. But the chief executive of SolarWinds on Wednesday gave a candid assessment of the company's supply chain compromise, apologizing for the way the company initially blamed the incident on an intern and providing new details about the timing of the attack.

Sudhakar Ramakrishna, the former CEO of Pulse Secure who took the top job at SolarWinds in January 2021, also said he was advised by friends and colleagues to "back out" of the company and find another job when it became clear around the time of his hiring that a supply chain attack targeting the company's Orion software had potentially infected thousands of organizations, including several government agencies.

Ramakrishna recounted an early conversation he had with William Bock, who sits on the company's board of directors, about his decision to stay on. "I felt that continuity and urgency was important in this situation. Having a new CEO come in… could be time consuming," he said. “I felt the right decision was to continue on as CEO given the needs of the company and customers.”

Similarly, when asked about Tim Brown, the company’s CISO since 2017, Ramakrishna said he wasn’t interested in making a scapegoat out of the security team. “I do not like to flog failures… While I acknowledge and accept that if you want to be an ‘action-oriented CEO,’ you fire a bunch of people, but I don’t think that does justice,” he said.

“Just as CEOs get a lot of credit when things go well… I think CISOs get undo discredit [when things go poorly], and I felt I should not be doing the norm or what is stereotypical in these situations, and went about my own way,” he added.

CISOs, CEOs, CIOs and other top executives at Target, Equifax, Uber, Capital One and several other companies have either resigned or been fired following security breaches in recent years. A common joke in the cybersecurity industry is that a CISO’s job is to be fired after such incidents.

SolarWinds CEO Sudhakar Ramakrishna at a February Congressional hearing.

Ramakrishna also apologized for the way the company blamed an intern for using a weak password—solarwinds123—during early testimony before congress. When asked about the password by Rep. Rashida Tlaib during a joint hearing by the House Oversight and Homeland Security committees, former SolarWinds CEO Kevin Thompson said the password was “a mistake that an intern made.” Ramakrishna also told lawmakers that the password was from an intern’s Github account.

“What happened at the congressional hearing where we attributed this to an intern was not appropriate and is not what we’re about,” Ramakrishna said during his RSA talk. “You want your employees, including interns, to make mistakes and learn from those mistakes and get better.”

On the topic of the breach itself, Ramakrishna also gave additional details about the timeline of the attack. The group behind the compromise, which the U.S. government has attributed to Russia’s foreign intelligence service, “may have been in our environment as early as jan 2019… doing very early recon activities,” Ramakrishna said. The company has said that it believed hackers initially accessed SolarWinds’ systems as early as September 2019.

Tags

- RSA
- SolarWinds
- supply chain attack
- SVR

Adam is the founding editor-in-chief of The Record by Recorded Future. He previously was the cybersecurity and privacy reporter for Protocol, and prior to that covered cybersecurity, AI, and other emerging technology for The Wall Street Journal.