SingCERT
Singapore Computer Emergency Response Team

Active Exploitation of Vulnerability in SolarWinds Orion Platform

Published on 14 Dec 2020

Updated on 23 Dec 2020

SolarWinds has issued a security advisory to address a "highly sophisticated supply chain attack" on its Orion Platform. There are reports of active exploits taking place. Many organisations have been affected globally, including reputed cybersecurity and technology companies such as FireEye, Microsoft and Cisco.

Successful exploitation of the vulnerability could allow attackers to gain access to vulnerable servers and perform malicious activities. Microsoft also observed that attackers abused their access by forging authentication tokens and impersonating existing users/administrators to evade detection.

Administrators are advised to disconnect or power down SolarWinds Orion products (running versions 2019.4 through 2020.2 HF1) from their network immediately. Administrators should also review the logs for suspicious activities, check connected systems for signs of compromise and persistence mechanisms, and reset credentials if necessary, especially ones used by or stored in SolarWinds software. Administrators are also advised to monitor their networks and systems for any suspicious activities.

SolarWinds has released a hotfix, Orion Platform version 2020.2.1 HF 2, to address the vulnerability. Administrators are advised to apply the hotfix as soon as possible.

Enterprises using products or services from affected technology companies should refer to the respective companies' websites for updates and recommended actions. Administrators are encouraged to visit these sites regularly to check for updates.

SolarWinds Resources:
https://www.solarwinds.com/securityadvisory
https://www.solarwinds.com/certadvisory
https://www.solarwinds.com/securityadvisory/faq
https://investors.solarwinds.com/financials/sec-filings/default.aspx

https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-security-vulnerability/

More information is available here:

https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaignleverages-software-supply-chain-compromise.html

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyberattacks/

https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

https://cyber.dhs.gov/ed/21-01/ https://us-cert.cisa.gov/ncas/alerts/aa20-352a

Last Updated 28 Dec 2020