EMBER365™ Security Bulletin

SolarWinds / FireEye Compromise

December 15, 2020

EMBER is aware of the global supply chain attack abusing SolarWinds® Orion® software. This high-severity, nation state attack enables Orion to distribute malware known as SUNBURST. The malware permits an attacker to gain access to network traffic management systems, making it possible for the attacker to gain elevated credentials. This compromise was used to target the cybersecurity firm FireEye, as well as multiple U.S. government agencies. For more information on the details of the breach, please see the advisory from the Cybersecurity & Infrastructure Security Agency.

EMBER and Client use of SolarWinds and FireEye products

EMBER **does not** use SolarWinds Orion or any FireEye product. We are unaware of the use of SolarWinds Orion, or any FireEye product, by any client we service. If you think you may be using SolarWinds Orion or any FireEye product without us knowing, or you're concerned about a partner or vendor you suspect or know is using the products, please contact us as quickly as possible.

EMBER **does** use SolarWinds MSP, an entirely different product, which is entirely unassociated with the Orion breach. SolarWinds MSP is a highly regarded remote management tool with a completely different code base. From SolarWinds: "We have also found no evidence that our SolarWinds MSP products, including RMM and N-central, and any of our free tools or agents contain the markers mentioned above." Reference: SolarWind's complete security advisory.

EMBER365 Managed Security Clients

If you are already protected by EMBER365, our complete managed threat detection and response service, we are monitoring your environment for any indications that it may be affected by this breach. In the event we observe any related activity, we will address it and notify you forthwith. If you have any questions or concerns, please contact us.

If you are not protected by EMBER365, this is a good time to learn more about threat detection and response and why it is imperative to every organization's cyber protection portfolio.

To learn more, go to: emberit.com/ember365

Additional Information

Microsoft Customer Guidance on Recent Nation-State Cyber Attacks

FireEye Threat Research

Homeland Security Cyber Emergency Directive 21-01

#END Bulletin