Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 25-20
Date: December 17, 2020
Phone: (202) 372-2904
E-Mail: CyberWatch@uscg.mil

URGENT NOTICE: ACTIVE EXPLOITATION OF POPULAR NETWORK MANAGEMENT SOFTWARE SOLARWINDS

SolarWinds recently reported a compromise of versions 2019.4 through 2020.2.1 HF1 of their Orion Platform by "a highly sophisticated, targeted, and manual supply chain attack by an outside nation state". The Orion Platform is a network management software used by numerous government agencies and approximately 300,000 additional customers worldwide. It is believed that malicious code was installed into software updates provided by SolarWinds to the platform's customers. Once the update was installed, it provided attackers access to the client's networks, allowing for elevated credential access, lateral movement throughout the network, and the ability to create other persistence mechanisms on devices and networks.

The Cybersecurity and Infrastructure Security Agency (CISA) has issued an Active Exploitation of Solar Winds Software alert, which includes multiple FireEye and SolarWinds advisories detailing potential countermeasures. CISA also issued Emergency Directive 21-01, which applies to federal agencies using SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, and provides a list of known Indicators of Compromise (IOC). The U.S. Coast Guard strongly urges all Marine Transportation System stakeholders using impacted versions of SolarWinds to take immediate actions to mitigate any risks of compromise.

As always, any potential threat to the cybersecurity of your vessel or facility should be taken seriously, and Breaches of Security or Suspicious Activities resulting from cyber incidents shall be reported to the National Response Center at 1-800-424-8802. For additional technical support, consider contacting the Coast Guard Cyber Command's 24x7 watch at 202-372-2904 or via email at CyberWatch@uscg.mil. Your willingness to comply and report in a timely manner helps the U.S. respond quickly and effectively and makes the maritime critical infrastructure safer.

Richard V. Timme, RDML, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends