DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

21 December 2021

MEMORANDUM FOR NAVSEA DEFENSE INDUSTRIAL BASE (DIB) PARTNERS

SUBJECT: SolarWinds Cyber Attack Information for NAVSEA Defense Industrial Base (DIB)

As you are likely aware, SolarWinds was the victim of a cyberattack which inserted a vulnerability (SUNBURST) into their Orion Platform. The Orion platform hosts eighteen distinct modules. A list of the affected modules can be found at the end of this document. This cyberattack on SolarWinds was very sophisticated. The attack occurred inside Solar Winds supply chain and once installed, requires manual intervention on the part of the malicious actor to compromise the underlying system. As such, this appears to be a targeted attack where the malicious actor casts a wide net then selects the most valuable targets to exploit. Needless to say, DoD, the Federal Government and you, our partners, were likely seen as high value targets.

Current threat analysis indicates that the SolarWinds.Orion.Core.BusinessLayer.dll was trojanized by malicious actors and once installed on a system or network, uses a backdoor to communicate via HTTP to third party web sites. The malware appears as the Orion Improvement Program (OIP) protocol, stores its reconnaissance results within legitimate SolarWinds files and includes the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The malware will attempt to resolve a subdomain of avsvmcloud[.]com to exfiltrate data. According to the the Department of Homeland Security (DHS) Computer Readiness Team (CERT) Emergency Directive 21-01, the vulnerable versions are:

Orion Platform 2019.4 HF5, version 2019.4.5200.9083

Orion Platform 2020.2 RC1, version 2020.2.100.12219

Orion Platform 2020.2 RC2, version 2020.2.5200.12394

Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

Due to the severity of this cyberattack, we encourage each of our DIB partners to examine their own networks to determine whether vulnerable SolarWinds software is installed. If vulnerable versions of SolarWinds Orion platform are installed on your networks or systems, we highly recommend you follow the directions in the DHS CERT Emergency 21-01 (https://cyber.dhs.gov/ed/21-01/#supplemental-guidance). This includes:

1. Disconnect or powering down affected assets

2. Forensically image system memory and/or operating systems of all affected assets. Analyze for new user or service accounts, privileged or otherwise.

2. Analyze stored network traffic for indications of compromise including new DNS entries.

4. Block all traffic to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed.

5. Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.

If analysis indicates a compromise of your SolarWinds Orion software, you are strongly encouraged to follow the post detection countermeasures listed on DHS Cybersecurity and Infrastructure Security Agency (CISA) page (https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software), and to follow the incident reporting requirements of the DFARS Clause 252.204-7012, should any network or system process, store or transmit Controlled Unclassified Information (CUI).

At this time, SolarWinds has not identified any other software versions as exploited or vulnerable.

List of affected SolarWinds Orion platform modules
- Application Centric Monitor (ACM)
- Database performance Analyzer Integration Module (DPAIM)
- Enterprise Operations Console (EOC)
- High Availability (HA)
- IP Address Manager (IPAM)
- Log Analyzer (LA)
- Network Automation Manager (NAM)
- Network Configuration Manager (NCM)
- Network Operations Manager (NOM)
- User Device Tracker (UDT)
- Network Performance Monitor (NPM)
- NetFlow Traffic Analyzer (NTA)
- Server & Application Monitor (SAM)
- Server Configuration Monitor (SCM)
- Storage Resource Monitor (SRM)
- Virtualization Manager (VMAN)
- VoIP & Network Quality Manager (VNQM)
- Web Performance Monitor (WPM)

The content of this communication does not authorize any change in the terms, conditions, delivery schedule, price, or amount of any government contracts.

NGUYEN.HUAN.TU.1184494961

Digitally signed by NGUYEN.HUAN.TU.1184494961
Date: 2020.12.21 16:35:30 -05'00'

H.T. NGUYEN
Deputy Commander
Cyber Engineering and Digital Transformation