GENERAL DYNAMICS
NASSCO

Inter-Department Memo

DATE: December 21, 2020

TO: Distribution

SUBJECT: General Dynamics NASSCO – Potential Cybersecurity Threat - SolarWinds Hack

FROM: NASSCO Cybersecurity Team

All General Dynamics NASSCO suppliers who utilize SolarWinds Orion software for their network management must be aware of the recent news by Cybersecurity & Infrastructure Security Agency (CISA) concerning a nation state hacking group who compromised the installation files of certain versions of the Orion application on the SolarWinds download site. See news article here: Active Exploitation of SolarWinds Software | CISA

You may also refer to SolarWinds Security Advisory FAQ site for more information. Security Advisory FAQ | SolarWinds

The federal government is directing all affected installations to be shut down or isolated from production network immediately. Network isolation can be accomplished through Endpoint Detection and Response (EDR) tools such as Carbon Black Response, Crowdstrike or others. This will prevent the server from communicating with any other machine on the network so that your incident responders can triage the incident.

There are a set of indicators (IOC's) that are published and constantly being updated as new information is being found about this hack. Please check these resources frequently and inspect your network for any signs of network activity, lateral movement or data exfiltration within your organization. GitHub - fireeye/sunburst_countermeasures

Furthermore, this site also publishes countermeasures which you can include in your security tools for additional protection.

Keep in mind if you do find evidence of network activity, lateral movement or data exfiltration within your organization you will be required by DFAR 252.204-7012 to report this incident to DoD DIBNET and General Dynamics NASSCO within 72 hours. Refer to instructions here: Defense Industrial Base Cybersecurity Information Sharing Program (dod.mil). You will need to purchase a medium assurance certificate to be able to post your incident (see details on the DoD DIBNET site above). Refer to General Dynamics NASSCO Supplier page for cyber security contact information GD NASSCO (nassco.com)

Also given the seriousness of this attack, your company may need to contract with outside agencies to perform forensics and other incident response activities. General Dynamics NASSCO cannot provide any company recommendations for this activity.

GENERAL DYNAMICS
NASSCO

To recover from this event, CISA is recommending that a new server be built, with a freshly installed OS and install an untainted version of SolarWinds including its database. Alternatively, a server snapshot can be restored from before the tainted version was installed. All user account passwords that have accessed the Orion server and any service accounts used by SolarWinds will need to be changed. Please check CISA's website for up-to-date guidance on remediation activities.

In any case, it is recommended to remain on high alert for any suspicious activity even after cleanup activities are completed.

For further questions, please contact our NASSCO Cybersecurity Team at cyber_report@nassco.com

# # #