NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

N★C DPS DEPARTMENT OF PUBLIC SAFETY

SolarWinds Incident Response Checklist

The below checklist was derived from U.S. CERT Advisory: AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations release December 17, 2020. **UPDATED 12/19/20**

Owners of vulnerable SolarWinds Orion products will generally fall into one of three categories:

• **Category 1** includes those who do not have the identified malicious binary. These owners can patch their systems and resume use as determined by and consistent with their internal risk evaluations. This category includes those versions which did **NOT** previously use an affected version (i.e., the instance was never rolled back from an affected version) and the instance is not restored from an affected version. Those organizations continuing to run instances of unaffected versions of SolarWinds Orion **must** comply with steps highlighted below.

• **Category 2** includes those who have identified the presence of the malicious binary—with or **without** beaconing to avsvmcloud[.]com. Owners with malicious binary whose vulnerable appliances only unexplained external communications are with avsvmcloud[.]com—a fact that can be verified by comprehensive network monitoring for the device—can harden the device, re-install the updated software from a verified software supply chain, and resume use as determined by and consistent with a thorough risk evaluation.

• **Category 3** includes those with the binary beaconing to avsvmcloud[.]com and secondary C2 activity to a separate domain or IP address. If you observed communications with avsvmcloud[.]com that appear to suddenly cease prior to December 14, 2020— not due to an action taken by your network defenders—you fall into this category. Assume the environment has been compromised, and initiate incident response procedures immediately.

Organizations that have the expertise to take the actions in Step 1 immediately should do so before proceeding to Step 2. Organizations without this capability should proceed to Step 2

SOLARWINDS ORION SPECIFIC MITIGATIONS

☐ **Step 1**

a. Forensically image system memory and/or host operating systems hosting all instances of affected versions of SolarWinds Orion. Analyze for new user or service accounts, privileged or otherwise.

b. Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections.

☐ **Step 2**

a. Affected organizations should immediately disconnect or power down affected all instances of affected versions of SolarWinds Orion from their network.

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

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

d. Follow the hardening guide at: Secure Configuration for the Orion Platform (solarwinds.com) with the following **EXCEPTIONS**:

1. Do **not** configure the SolarWinds software to implement SAML-based authentication that relies on Microsoft's Active Directory Federated Services. This configuration is currently

being exploited by the threat actor associated with this activity.

2. Do **not** follow the hardening guideline's requirement to ensure their SolarWinds instance is patched to the latest version, pending further direction from CISA to do so. (If applicable)

□ **Step 3**

Only after all known threat actor-controlled accounts and persistence mechanisms have been removed:

- □ Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that the threat actor has deployed further persistence mechanisms.
- □ Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.
- □ Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
- □ Take actions to remediate kerberoasting, including—as necessary or appropriate—engaging with a third party with experience eradicating APTs from enterprise networks. For Windows environments, refer to the following Microsoft's documentation on kerberoasting: https://techcommunity.microsoft.com/t5/microsoft-security-and/detecting-ldap-based-kerberoasting-with-azure-atp/ba-p/462448.
- □ Require use of multi-factor authentication. If not possible, use long and complex passwords (greater than 25 characters) for service principal accounts, and implement a good rotation policy for these passwords.
- □ Replace the user account by group Managed Service Account (gMSA), and implement Group Managed Service Accounts: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview.
- □ Set account options for service accounts to support AES256_CTS_HMAC_SHA1_96 and not support DES, RC4, or AES128 bit encryption.
- □ Define the Security Policy setting for Network Security: Configure Encryption types allowed for Kerberos. Set the allowable encryption types to AES256_HMAC_SHA1 and Future encryption types: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos.
- □ See Microsoft's documentation on how to reset the Kerberos Ticket Granting Ticket password twice: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password
- □ Send all SolarWinds logs to a centralized logging solution e.g. SIEM and/Security Operations Center (SOC).

AFFECTED SOLARWINDS ORION PRODUCTS

Orion Platform Version	**Sunburst Backdoor Code Present**	**File Version**	**SHA-256**
2019.4	**Tampered but not backdoored**	2019.4.5200.8890	a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
2019.4 HF1	No	2019.4.5200.8950	9bee4af53a8cdd7ecabe5d0c77b6011abe887ac516a5a22ad51a058830403690
2019.4 HF2	No	2019.4.5200.8996	bb86f66d11592e3312cd03423b754f7337aeebba9204f54b745ed3821de6252d
2019.4 HF3	No	2019.4.5200.9001	ae6694fd12679891d95b427444466f186bcdcc79bc0627b590e0cb40de1928ad

Orion Platform Version	Sunburst Backdoor Code Present	File Version	SHA-256
2019.4 HF4	No	2019.4.5200.9045	9d6285db647e7eeabdb85b409fad61467de1655098fec2e25aeb7770299e9fee
2020.2 RC1	**Yes**	2020.2.100.12219	dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
2019.4 HF5	**Yes**	2019.4.5200.9083	32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
2020.2 RC2	**Yes**	2020.2.5200.12394	019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
2020.2 2020.2 HF1	**Yes**	2020.2.5300.12432	ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
2019.4 HF6	No	2019.4.5200.9106	8dfe613b00d495fb8905bdf6e1317d3e3ac1f63a626032fa2bdad4750887ee8a
2020.2.1 2020.2.1 HF1	No	2020.2.15300.12766	143632672dcb6ef324343739636b984f5c52ece0e078cfee7c6cac4a3545403a

MICROSOFT PROACTIVE MEASURES

Privilege Escalation and Persistence [TA0004, TA0003]

The adversary has been observed using multiple persistence mechanisms across a variety of intrusions. CISA has observed the threat actor adding authentication tokens and credentials to highly privileged Active Directory domain accounts as a persistence and escalation mechanism. In many instances, the tokens enable access to both on-premise and hosted resources. Microsoft has released a query that can help detect this activity.[4] [Note: Requires the use of Microsoft Azure Sentinel]

Microsoft reported that the actor has added new federation trusts to existing infrastructure, a technique that CISA believes was utilized by a threat actor in an incident to which CISA has responded. Where this technique is used, it is possible that authentication can occur outside of an organization’s known infrastructure and may not be visible to the legitimate system owner. Microsoft has released a query to help identify this activity.[5] Note: Requires the use of Microsoft Azure Sentinel]

ADDITIONAL MEASURES

Operational Security

Due to the nature of this pattern of adversary activity—and the targeting of key personnel, incident response staff, and IT email accounts—discussion of findings and mitigations should be considered very sensitive, and should be protected by operational security measures. An operational security plan needs to be developed and socialized, via out-of-band communications, to ensure all staff are aware of the applicable handling caveats.

Operational security plans should include:

- Out-of-band communications guidance for staff and leadership;
- An outline of what “normal business” is acceptable to be conducted on the suspect network;

- A call tree for critical contacts and decision making; and
- Considerations for external communications to stakeholders and media