DIR OCISO

Office of the
Chief Information
Security Officer
State of Texas

TLP: WHITE

Distribution Limits

TLP: **WHITE** = Disclosure is not limited.

The materials provided are for information only. Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any 3rd party views and opinions do not necessarily reflect those of DIR or its employees. By sharing this material, DIR does not endorse any particular person, entity, product or service.

SUBJECT: Updated Recommendations on SolarWinds Orion Hot Fix Release and Supporting Actions

TLP: WHITE

DATE: Dec 18, 2020

The Texas Department of Information Resources (DIR) is issuing additional guidance on the use of SolarWinds Orion products. It is incumbent on each organization to thoroughly evaluate their risk category based on the categorical guidance in CISA's Activity Alert AA20-352A - *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, and the additional context provided by DIR.

DHS CISA identifies the following SolarWinds Orion version as impacted:

- 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

Organizational Risk Assessment

CISA's Activity Alert AA20-352A categorizes the organizations who were running a vulnerable version of SolarWinds Orion products to generally fall into one of three categories.

Category 1

Includes those who do not have the identified malicious binary. CISA's Activity Alert states that owners can patch their systems and resume use as determined by and consistent with their internal risk evaluations.

Category 2

Includes those who have identified the presence of the malicious binary, with or without beaconing to avsvmcloud[.]com. CISA's Activity Alert states that owners with malicious binary whose vulnerable appliance's 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.

- DIR has additional guidance to support the determination if your organization meets the threshold of Category 2:
    - Determine how far back your organization's logs cover.
    - Do your organization's logs go back at least 6 months (to May or June 2020) and are they clear of any beaconing or IOC?
    - If no evidence of beaconing, consider patching the server to the latest Hot Fix and continue to monitor the environment and consider additional capacity for longer log retention.
    - If organizations are unable to review 6 months of log data, consider your organization in Category 3 out of an abundance of caution.

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.

Recommendations

Recommended reinstallation process:

1. If you have not rebuilt or patched your server, from an isolated environment take a forensics image of each server. Save this image for potential further investigation and analysis.
2. Conduct appropriate analysis of the environment, including:
    a. Analyze the server for any new user or service accounts, privileged or otherwise.
    b. Analyze the firewall, VPN, or any other ingress/egress points to that box back to the time the affected patch was applied.
    c. If you don't have logs that go back to the date of the update, you can't verify there wasn't a call out.

    d. If your organization does not have adequate forensic experience, please see the Forensic Resources section below.

3. Install the appropriate SolarWinds Orion version, after appropriate testing prior to pushing the changes to a production environment and confirm the appropriate vendor recommended security configurations.
4. If available, ensure the latest Indicators of Compromise are configured in your Endpoint Detection and Response (EDR) solution. If your organization does not have an EDR solution, enable Windows Defender in applicable Microsoft systems.

Organizations should be aware of the threat of ongoing vulnerabilities and should continue to monitor their network for malicious activity.

Forensic Resources

Organizations that do not have forensics capability that have affected servers and need analysis can get this service through the DIR Managed Security Services (MSS) contract.

- State Agencies, Institutions of Higher Education, or Junior Colleges may contact DIRSharedServices@dir.texas.gov to obtain assistance from DIR MSS.
- Local organizations may also leverage the DIR MSS contract by calling 877-DIR-CISO or (877) 347-2476.
- Please be aware there is a cost involved with leveraging MSS Resources.
- A forensic image capture guide is available from MS-ISAC, if you need this document, please reach out to SOC@cisecurity.org or DIRSecurity@dir.texas.gov.

References

- CISA Activity Alert AA20-352A
- SolarWinds FAQ
- NSA Advisory on Detecting Abuse of Authentication Mechanisms

TLP: WHITE

Sources may use TLP: **WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: **WHITE** information may be distributed without restriction.

https://www.us-cert.gov/tlp

DIR.TEXAS.GOV

Assistance/Feedback/Questions?

Office of the Chief Information Security Officer

DIRSecurity@dir.texas.gov

Texas Department of Information Resources

Transforming How Texas Government Serves Texans