Office of the
Chief Information Security Officer
State of Texas

TLP: GREEN

Distribution Limits

TLP: GREEN = Limited disclosure, restricted to the community

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: Urgent Notification: Recommended Mitigation of SolarWinds Orion Platform Compromise

TLP: GREEN

DATE: Dec 14, 2020

The Texas Department of Information Resources is actively engaged with our federal, state, and industry partners to ensure cybersecurity in Texas. We are evaluating the matter as more information becomes available and are taking all available security measures.

In response the federal Cybersecurity and Infrastructure Security Agency (CISA) has published an urgent Current Activity Alert: Active Exploitation of SolarWinds Software and Emergency Directive 21-01, "*Mitigate SolarWinds Orion Code Compromise, "*directed at Federal Civilian Agencies, further emphasizing the urgency of this Alert: https://cyber.dhs.gov/ed/21-01/

In alignment with CISA Emergency Directive 21-01, DIR recommends all instances of SolarWinds Orion Platform software versions 2019.4 through 2020.2.1 **be isolated and shut down as soon as possible**.

RECOMMENDED IMMEDIATE ACTIONS

2. Immediately **disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from your network**.
3. **Block all traffic** to and from hosts, external to the enterprise, where *any version of* SolarWinds Orion software has been installed.
4. If you have the capability, forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1.
5. Analyze your network for new user or service accounts, privileged or otherwise.
6. 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.
7. Configure your anti-malware and intrusion detection and prevention systems to block the following:
    1. File hashes:
        MD5: b91ce2fa41029f6955bff20079468448
        SHA256:
        32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
    2. Internet Indicators:
        Domain: acsvmcloud[.]com
        URL: /swip/Events
        String: OrionImprovementBusinessLayer
        Named Pipe: 583da945-62af-10e8-4902-a8f205c72b2e

UNTIL FURTHER NOTICE, WE ALSO RECOMMEND YOU

1. Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed.
2. Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.
3. Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
4. Take actions to remediate kerberoasting, including, as necessary or appropriate, engaging with a 3rd party with experience eradicating APTs from enterprise networks. For Windows environments, refer to the following:
    - See 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 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). See https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview 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

FOR MORE INFORMATION, VISIT

1. SolarWinds Security Advisory
2. FireEye Advisory: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor
3. FireEye GitHub page: Sunburst Countermeasures
4. Microsoft Advisory

REPORTING

We also recommend you report to DIR via the ISAO Threat Reporting Form and quarantine the following:

a. SolarWinds.Orion.Core.BusinessLayer.dll with a file hash of b91ce2fa41029f6955bff20079468448

b. C:\WINDOWS\SysWOW64\netsetupsvc.dll

If you have evidence of impacts related to this issue, please call the DIR OCISO on-call number at 877-DIR-CISO (347-2476).

TLP: GREEN

Recipients may share TLP: **GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:**GREEN** information may not be released outside of the community.

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