Emergency Directive 21-01

December 13, 2020

Mitigate SolarWinds Orion Code Compromise

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency’s Emergency Directive 21-01, “Mitigate SolarWinds Orion Code Compromise”.

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to “issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.” 44 U.S.C. § 3553(h)(1)-(2).

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3).

Federal agencies are required to comply with these directives. 44 U.S.C. § 3554(a)(1)(B)(v).

These directives do not apply to statutorily-defined “national security systems” nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).

Background

SolarWinds Orion products (affected versions are 2019.4 through 2020.2.1 HF1) are currently being exploited by malicious actors. This tactic permits an attacker to gain access to network traffic management systems. Disconnecting affected devices, as described below in Required Action 2, is the only known mitigation measure currently available.

CISA has determined that this exploitation of SolarWinds products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. This determination is based on:

- Current exploitation of affected products and their widespread use to monitor traffic on major federal network systems;
- High potential for a compromise of agency information systems;
- Grave impact of a successful compromise.

CISA understands that the vendor is working to provide updated software patches. However, agencies must wait until CISA provides further guidance before using any forthcoming patches to reinstall the SolarWinds Orion software in their enterprise.

Please refer to the MITRE ATT&CK framework for possible tactics the threat actors are using to maintain persistence in the environment.
Required Actions

This emergency directive requires the following actions:

1. Agencies that have the expertise to take the following actions immediately must do so before proceeding to Action 2. Agencies without this capability shall proceed to Action 2.
   a. Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1. 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.

2. Affected agencies shall immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network. Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package, agencies are prohibited from (re)joining the Windows host OS to the enterprise domain. Affected entities should expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available. Additionally:
   a. Block all traffic to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed.
   b. Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.

3. By 12pm Eastern Standard Time on Monday December 14, 2020 agencies shall report as an incident to CISA (at https://us-cert.cisa.gov/report) the existence of any of the following:
   b. [C:\WINDOWS\SysWOW64\netsetupsvc.dll]
   c. Other indicators related to this issue to be shared by CISA

4. After (and only after) all threat actor-controlled accounts and identified persistence mechanisms have been removed:
   a. Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed.
   b. Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.
   c. Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
   d. 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:
      - 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.


• See Microsoft’s documentation on how to reset the Kerberos Ticket Granting Ticket password, twice: https://docs.microsoft.com/en-us/windows-server/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos

5. By 12pm Eastern Standard Time on Monday December 14, 2020, submit a report to CISA using the provided template. Department-level Chief Information Officers (CIOs) or equivalents must submit completion reports attesting to CISA that the affected devices were either disconnected or powered down.

These requirements apply to any agency network utilizing the SolarWinds Orion product. This includes any information system used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information.

CISA Actions

• CISA will continue to work with our partners to monitor for active exploitation associated with this vulnerability. CISA will release additional indicators of compromise as they become available.

• CISA will provide additional guidance to agencies via the CISA website, through an emergency directive issuance coordination call, and through individual engagements upon request (via CyberDirectives@cisa.dhs.gov).

Duration

This emergency directive remains in effect until all agencies have applied the forthcoming patch or the directive is terminated through other appropriate action.

Additional Information

• General information, assistance, and reporting – CyberDirectives@cisa.dhs.gov
• Reporting indications of potential compromise – Central@cisa.dhs.gov

Supplemental Guidance

December 18, 2020

This section provides additional guidance on the implementation of CISA Emergency Directive (ED) 21-01, to include an update on affected versions, guidance for agencies using third-party service providers, and additional clarity on required actions. On December 13, 2020, CISA issued ED 21-01 to mitigate the SolarWinds Orion Code Compromise. As noted in ED 21-01, CISA continues to work with our partners to monitor for active
exploitation associated with this compromise and will continue providing updated guidance to agencies as new information becomes available. ED 21-01 also indicated that agencies must wait until CISA provides further guidance before using any forthcoming patches to reinstall the SolarWinds Orion software in their enterprise. This supplemental guidance is the first in that series of guidance. CISA will continue to provide further guidance as new information becomes available.

ED 21-01 directed agencies to immediately disconnect or power down SolarWinds Orion, versions 2019.4 through 2020.2.1 HF1, from their network. As of this guidance and based on developing information, CISA is dividing this range of versions into two groups: versions that have been identified as containing a malicious backdoor ("affected versions") and versions that have been identified as not containing that malicious backdoor ("unaffected versions"). ED 21-01 and this guidance also contain instructions relating to versions of SolarWinds Orion outside of this version range ("other versions").

Affected Versions

The following versions are considered affected versions:

- 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

Agencies that were using affected versions at any time prior to the issuance of ED 21-01 must:

1. **Keep these products disconnected** as required by ED 21-01 pending further CISA guidance and not rebuild or reimage the affected platforms and host operating systems (OS), including (re)joining the host OS to the enterprise domain, until such time as CISA directs otherwise.

2. Label and isolate all backups of the affected versions from their systems to prevent accidental reintroduction of malicious code to the production environment.

3. Conduct forensic analysis or search, as appropriate based on capability, for indicators of compromise (IOCs) or other evidence of threat actor activity.
   
   a. Agencies running affected versions that have no capability to conduct forensic analysis (system memory, host storage, network) shall, at minimum, search for IOCs or other evidence of threat actor activity published in ED 21-01, Activity Alert AA20-352A, and future associated guidance.

   b. Agencies that find matches to these IOCs or evidence of threat actor activity through forensics analysis must report this as an incident to CISA through https://us-cert.cisa.gov/report. If a reporting agency already submitted incident information to CISA, please send updates to CISA as you discover new evidence.

   c. Agencies running affected versions that have no capability to conduct forensic analysis and no capability to search for IOCs shall assume breach, report the incident to CISA through https://us-cert.cisa.gov/report, and contact central@cisa.dhs.gov to coordinate finding a qualified service provider capable of conducting forensics.

*All other provisions specified in ED 21-01 remain in effect.*

**Federal Information Systems Hosted in Third-Party Environments (such as Cloud)**

CISA is working closely with FedRAMP to coordinate the response to ED 21-01 with FedRAMP Authorized cloud service providers (CSPs). FedRAMP Authorized CSPs have been informed to coordinate with their
agency customers.

1. If FedRAMP Authorized CSPs are affected, their agency customers must report incidents to CISA in accordance with ED 21-01. Agencies hosting information in any third-party environment (FedRAMP Authorized or otherwise) must identify and contact their third-party service providers directly for status pertaining to, and to ensure compliance with, ED 21-01.

2. Agencies are also instructed to supplement their reporting under ED 21-01 to incorporate relevant information from third-party service providers (to the extent that agencies have not already included this information), including to report any incident through CISA. In your incident reporting, please identify what data was exposed to the third-party service provider.

Conditions for Reconnecting Unaffected Versions

At this time, CISA is still assessing whether it is appropriate to relax ED 21-01’s requirement that agencies not install patches for their SolarWinds Orion software. Some older versions of SolarWinds Orion have been identified as not affected by the malicious backdoor. However, operating such older versions carries significant risk, because (1) like other types of older software, older versions of SolarWinds Orion contain known vulnerabilities; (2) the adversary that inserted the SolarWinds Orion backdoor is likely to be intimately familiar with SolarWinds Orion code, including known or unknown vulnerabilities that may exist separate and apart from the backdoor; and (3) this adversary has demonstrated the capability and willingness to exploit SolarWinds Orion to compromise U.S. government agencies, critical infrastructure entities, and private organizations.

Agencies are permitted to power back up and reintroduce into an agency production environment SolarWinds Orion instances that were disconnected pursuant to ED 21-01 only if each of the following conditions are met:

1. The instance currently uses an unaffected version of the SolarWinds Orion, which are listed below.
   a. Orion Platform 2019.4 2019.4.5200.8890
   b. Orion Platform 2019.4 HF1 2019.4.5200.8950
   c. Orion Platform 2019.4 HF2 2019.4.5200.8996
   d. Orion Platform 2019.4 HF3 2019.4.5200.9001
   e. Orion Platform 2019.4 HF4 2019.4.5200.9045

2. The instance 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.

3. The agency first (1) hunts for threat actors in their environment using all IOCs and indicators of threat actor activity published about this threat activity in ED 21-01, Activity Alert AA20-352A, and any additional related guidance related to this activity published by CISA or provided by the information security community prior to the instance being reintroduced to the environment, and (2) finds no evidence of such threat actor activity.

4. The agency conducts a risk assessment to assess the impact of reintroducing the Orion Platform into agency production environments and accepts residual risk associated with running this unpatched software containing known vulnerabilities until such time as CISA permits agencies to patch these products.

5. Block all incoming and outgoing (any:any) Internet traffic to and from hosts running SolarWinds Orion products (as required by ED 21-01).
6. Follow the SolarWinds hardening guidelines provided by the vendor, which can be found at: https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-secure-configuration.htm

EXCEPT:

a. Agencies shall **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.

b. Agencies shall **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.

7. Ensure that the SolarWinds logs are being sent to the agency SOC for action.

**Other Versions**

Agencies continuing to run instances of SolarWinds Orion with other versions **must** comply with steps 5-7 listed for unaffected versions.

Agencies may apply updates to host operating system running SolarWinds Orion products in accordance with their respective vulnerability and patch management policies and programs.

*All other provisions specified in ED 21-01 remain in effect.*

**Frequently Asked Questions**

Answers to common questions appear below.

- **What does the directive mean by “expertise”?**
- **What does the supplemental guidance mean by “disconnected”?**

**What does the directive mean by “expertise”?**

By “expertise”, we mean that you have staff or supporting personnel that are properly trained in taking a forensic image of system memory and have tooling readily-available to immediately do so.

**What does the supplemental guidance mean by “disconnected”?**

By “disconnected” we mean *disconnected from the network and powered on* if the agency has the capability- or is seeking a capable service provider- to collect forensics images (system memory, host storage, network) off of the host or virtual machine, or *disconnected from the network and powered off* if there is no such capability.
JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

Original release date: December 16, 2020

Over the course of the past several days, the FBI, CISA, and ODNI have become aware of a significant and ongoing cybersecurity campaign. Pursuant to Presidential Policy Directive (PPD) 41, the FBI, CISA, and ODNI have formed a Cyber Unified Coordination Group (UCG) to coordinate a whole-of-government response to this significant cyber incident. The UCG is intended to unify the individual efforts of these agencies as they focus on their separate responsibilities. This is a developing situation, and while we continue to work to understand the full extent of this campaign, we know this compromise has affected networks within the federal government.

As the lead for threat response, the FBI is investigating and gathering intelligence in order to attribute, pursue, and disrupt the responsible threat actors. The FBI is engaging with known and suspected victims, and information gained through FBI’s efforts will provide indicators to network defenders and intelligence to our government partners to enable further action.

As the lead for asset response activities, CISA took immediate action and issued an Emergency Directive instructing federal civilian agencies to immediately disconnect or power down affected SolarWinds Orion products from their network. CISA remains in regular contact with our government, private sector and international partners, providing technical assistance upon request.
and making needed information and resources available to help those affected recover from this incident. CISA is engaging with our public and private stakeholders across the critical infrastructure community to ensure they understand their exposure and are taking steps to identify and mitigate any compromises.

As the lead for intelligence support and related activities, ODNI is helping to marshal all of the Intelligence Community’s relevant resources to support this effort and share information across the United States Government.

To report suspicious or criminal activity related to information found in this statement, contact your local FBI field office at www.fbi.gov/contact-us/field. To request incident response resources or technical assistance related to this statement, visit https://www.us-cert.gov/report or email Central@cisa.gov.

---

**Topics:** Cybersecurity

**Keywords:** Cybersecurity

**Last Published Date:** December 16, 2020

---

TLP:WHITE

TLP:WHITE