Emergency Directive 21-01 - Supplemental Guidance v. 1 - Mitigate SolarWinds Orion Code Compromise

Original Release Date: December 18, 2020

This document provides additional guidance on the implementation of CISA Emergency Directive 21-01, to include an update on affected versions, guidance for agencies using third-party service providers, and additional clarity on required actions.

FROM: Brandon Wales, Acting Director,
Cybersecurity and Infrastructure Security Agency, Department of Homeland Security

CC: Russell T. Vought, Director,
Office of Management and Budget

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

This document 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
- Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

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

1. **Keep these products disconnected**[1] 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 re-introduction 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 (https://us-cert.cisa.gov/ncas/alerts/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

[1] 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.

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 (https://us-cert.cisa.gov/report). 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. Affected versions are listed again here for convenience.
    a) Orion Platform 2019.4 HF5, version 2019.4.5200.9083
    b) Orion Platform 2020.2 RC1, version 2020.2.100.12219
    c) Orion Platform 2020.2 RC2, version 2020.2.5200.12394
    d) Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

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 (https://us-cert.cisa.gov/ncas/alerts/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.

Agencies should 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.

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.

CISA Actions

- CISA will continue to work with our partners to monitor for active exploitation associated with this vulnerability. CISA will release additional IOCs 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).

Additional Information

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