SUPPLY CHAIN COMPROMISE

CISA is tracking a significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations. An advanced persistent threat (APT) actor is responsible for compromising the SolarWinds Orion software supply chain, as well as widespread abuse of commonly used authentication mechanisms. This threat actor has the resources, patience, and expertise to gain access to and privileges over highly sensitive information if left unchecked. CISA urges organizations to prioritize measures to identify and address this threat.

Pursuant to Presidential Policy Directive (PPD) 41, CISA, the Federal Bureau of Investigation (FBI) and the Office of the Director of National Intelligence (ODNI) have formed a Cyber Unified Coordination Group (UCG) to coordinate a whole-of-government response to this significant cyber incident.

CISA also remains in regular contact with public and private sector stakeholders and international partners, providing technical assistance upon request, and making information and resources available to help those affected to recover quickly from incidents related to this campaign.

CISA encourages individuals and organizations to refer to the resources below for additional information on this compromise. These resources provide information to help organizations detect and prevent this activity.

Collapse All Sections

Emergency Directive and Updates

- CISA Emergency Directive 21-01
  - CISA has determined that this exploitation of SolarWinds products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. Multiple versions of SolarWinds Orion 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 in Required Action 2 of the ED, is the only known mitigation measure currently available.

- CISA Supplemental Guidance on Emergency Directive 21-01
    - On December 18, 2020, CISA's supplemental release provides additional guidance on the implementation of ED 21-01, to include an update on affected versions, guidance for agencies using third-party service providers, and additional clarity on required actions.

Press Releases

- 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)
    - This Joint Statement announces establishment of a Cyber Unified Coordination Group (UCG). Pursuant to Presidential Policy Directive (PPD) 41, FBI, CISA, and ODNI have formed a 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.
- CISA Press Release: CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products
    - This press release announces the CISA Emergency Directive 21-01 in response to the known compromise involving SolarWinds Orion products. The ED calls on federal civilian agencies to review their networks for IOCs and disconnect or power down SolarWinds Orion Products immediately. This is the fifth Emergency Directive issued by CISA under the authorities granted by Congress in the Cybersecurity Act of 2015.

Alerts and Guidance

- CISA Releases Free Detection Tool for Azure/M365 Environment
    - CISA has created a free tool for detecting unusual and potentially malicious activity that threatens users and applications in an Azure/Microsoft O365 environment. The tool is intended for use by incident responders and is narrowly focused on activity that is endemic to the recent identity- and authentication-based attacks seen in multiple sectors.
- CISA Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
    - This Alert provides technical details, indicators of compromise, and mitigations for the ongoing compromise by the APT actor. This threat actor has demonstrated sophistication and complex tradecraft in these intrusions. CISA expects that removing the threat actor from compromised environments will be highly complex and challenging. It is likely that the adversary has additional initial access vectors and TTPs that have not yet been discovered. CISA will continue to update this Alert and the corresponding indicators of compromise (IOCs) as new information becomes available.
- CISA Insights: What Every Leader Needs to Know About the Ongoing Cyber Incident

- This CISA Insights complements CISA Alert AA20-352A and is geared toward C-suite leadership. It details the risk posed by the ongoing cyber incident and provides immediate actions that executives can take to assess the risk posed to their organization and enhance their operational security.

Partner Products

- NSA Cybersecurity Advisory: Detecting Abuse of Authentication Mechanisms
  - This NSA cybersecurity advisory describes tactics, techniques, and procedures used by malicious cyber actors to access protected data in the cloud and provides guidance on defending against and detecting such activity.
- SolarWinds Security Advisory
  - This SolarWinds advisory describes the cyberattack to their system that inserted the SUBURST vulnerability within the Orion Platform software builds, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.
- FireEye Advisory: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
  - This FireEye advisory addresses the supply chain attack trojanizing SolarWinds Orion Business software updates in order to distribute malware referred to as “SUNBURST.”
- FireEye GitHub Page: Sunburst Countermeasures
  - The FireEye GitHub repository provides rules in multiple languages (Snort, Yara, IOC, ClamAV) to detect the threat actor and supply chain attacks in the wild.