Supply Chain Compromise | CISA

Published: 2021-01-07 · Archived: 2026-04-10 02:43:06 UTC

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.

CISA Hunt and Incident Response Program (CHIRP)

CISA released the CISA Hunt and Incident Response Program (CHIRP), a forensics collection capability outlined in Activity Alert AA21-077A and available on CISA's CHIRP GitHub repository. This capability was developed to assist network defenders with detecting advanced persistent threat (APT) activity related to the SolarWinds and Active Directory/M365 compromise. The initial release of CHIRP scans for signs of APT compromise within an on-premises environment to detect indicators of compromise (IOCs) associated with CISA Alerts AA20-352A and AA21-008A.

Emergency Directive and Update

On January 6, 2021, CISA Released Supplemental Guidance on Emergency Directive 21-01 that requires (1) agencies that ran affected versions conduct forensic analysis, (2) agencies that accept the risk of running SolarWinds Orion comply with certain hardening requirements, and (3) reporting by agency from department-level Chief Information Officers (CIOs) by Tuesday, January 19, and Monday, January 25, 2020.

Press Releases

- Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)

    - On behalf of President Trump, the National Security Council staff has stood up a task force construct known as the Cyber Unified Coordination Group (UCG), composed of the FBI, CISA, and ODNI with support from NSA, to coordinate the investigation and remediation of this significant cyber incident involving federal government networks. The UCG is still working to understand the scope of the incident but has the following updates on its investigative and mitigation efforts.
- 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.

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.

Alerts and Guidance

CISA's Alerts and Advisories provides more information about this and related cyber incidents.
