Supply Chain Compromise

cisa.gov/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.

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.

A demonstration video is available on CISA's YouTube channel to help agencies and organizations understand how to use CHIRP.

Emergency Directive and Updates

- CISA Updates Supplemental Guidance on Emergency Directive 21-01
  On January 6, 2021, CISA released supplemental guidance v3 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.
- CISA Updates Supplemental Guidance on Emergency Directive 21-01
  On December 30, 2020, CISA released guidance to supplement the Emergency Directive (ED) 21-01 and Supplemental Guidance v1 issued on December 18, 2020. Specifically, all federal agencies operating versions of the SolarWinds Orion platform other than those identified as "affected versions" are required to use at least SolarWinds Orion Platform version 2020.2.1HF2.
- 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.
- CISA Emergency Directive 21-01
  On December 13, 2020 CISA 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.

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.

Alerts and Guidance

- CISA, alongside the United Kingdom's National Cyber Security Centre, FBI and NSA published an advisory to provide further details of tactics, techniques and procedures (TTPs) associated with SVR cyber actors. CISA has also released Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise that provides summaries of three key joint publications that focus on SVR activities related to the SolarWinds Orion supply chain compromise.
- Malware Analysis Report (AR21-105A) was published April 15. This report provides detailed analysis of several malicious samples and artifacts associated with the supply chain compromise of SolarWinds Orion network management software, attributed by the U.S. Government to the Russian SVR Foreign Intelligence Service (APT 29, Cozy Bear, The Dukes). CISA and CNMF are distributing this MAR to enable network defense and reduced exposure to malicious activity. This MAR includes suggested response actions and recommended mitigation techniques.
- On April 15, the United States formally named the Russian Foreign Intelligence Service (SVR) as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. Additional information may be found in a fact sheet from the White House.
- CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on Russian Foreign Intelligence Service (SVR) actors scanning for and exploiting vulnerabilities to compromise U.S. and allied networks, including national security and government-related systems.

- 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.
- CISA has published a table of tactics, techniques, and procedures (TTPs) used by the advanced persistent threat (APT) actor involved with the recent SolarWinds Orion supply chain compromise. The table uses the MITRE ATT&CK framework to identify APT TTPs and includes detection recommendations. This information will assist network defenders in detecting and responding to this activity.
- CISA is providing guidance on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise to support federal departments and agencies in evicting this threat activity from compromised on-premises and cloud environments. This guidance addresses tactics, techniques, and procedures (TTPs) leveraged by the threat actor.
- CISA Insights: SolarWinds and AD-M365 Compromise Risk Decisions for Leaders
  This CISA Insights will help executive leaders of affected entities understand and be able to articulate the threat, risk, and associated actions their organizations should take.
- CISA encourages affected organizations to review and apply the necessary guidance in the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page and CISA Insights.
- MAR-10318845-1.v1 - SUNBURST | CISA This report provides detailed analysis of several malicious artifacts associated with a sophisticated supply chain compromise of SolarWinds Orion network management software, identified by the security company FireEye as SUNBURST.
- MAR-10320115-1.v1 - TEARDROP | CISA This report provides detailed analysis of malicious artifacts associated with a sophisticated supply chain compromise of Solar Winds Orion network management software, identified by the security company FireEye as TEARDROP.
- CISA Releases New Alert on Post-Compromise Threat Activity in Microsoft Cloud Environments and Tools to Help Detect This Activity
  CISA has evidence of post-compromise advanced persistent threat (APT) activity in the cloud environment. Specifically, CISA has seen an APT actor using compromised applications in a victim's Microsoft 365 (M365)/Azure environment and using additional credentials and Application Programming Interface (API) access to cloud resources of private and public sector organizations. This activity is in addition to what has been previously detailed in AA20-352A.
- CISA Releases Emergency Directive (ED) 21-01 Supplemental Guidance Version 3: Mitigate SolarWinds Orion Code Compromise.
  This Alert provides guidance that supersedes Required Action 4 of ED 21-01 and Supplemental Guidance versions 1 and 2.

- 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.

DHS and CISA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS or CISA.

Was this webpage helpful? Yes | Somewhat | No