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) | CISA

Published: 2021-01-05 · Archived: 2026-04-05 16:24:39 UTC

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.

This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort. We are taking all necessary steps to understand the full scope of this campaign and respond accordingly.

The UCG believes that, of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number have been compromised by follow-on activity on their systems. We have so far identified fewer than ten U.S. government agencies that fall into this category, and are working to identify and notify the nongovernment entities who also may be impacted.

This is a serious compromise that will require a sustained and dedicated effort to remediate. Since its initial discovery, the UCG, including hardworking professionals across the United States Government, as well as our private sector partners have been working non-stop. These efforts did not let up through the holidays. The UCG will continue taking every necessary action to investigate, remediate, and share information with our partners and the American people.

As the lead agency for threat response, the FBI's investigation is presently focused on four critical lines of effort: identifying victims, collecting evidence, analyzing the evidence to determine further attribution, and sharing results with our government and private sector partners to inform operations, the intelligence picture, and network defense.

As the lead for asset response, CISA is focused on sharing information quickly with our government and private sector partners as we work to understand the extent of this campaign and the level of exploitation. CISA has also created a free tool for detecting unusual and potentially malicious activity related to this incident. In an Emergency Directive posted December 14, CISA directed the rapid disconnect or power-down of affected SolarWinds Orion products from federal networks. CISA also issued a technical alert providing technical details and mitigation strategies to help network defenders take immediate action. CISA will continue to share any known details as they become available.

As the lead for intelligence support and related activities, ODNI is coordinating the Intelligence Community to ensure the UCG has the most up-to-date intelligence to drive United States Government mitigation and response activities. Further, as part of its information-sharing mission, ODNI is providing situational awareness for key stakeholders and coordinating intelligence collection activities to address knowledge gaps.

Lastly, the NSA is supporting the UCG by providing intelligence, cybersecurity expertise, and actionable guidance to the UCG partners, as well as National Security Systems, Department of Defense, and Defense Industrial Base system owners. NSA's engagement with both the UCG and industry partners is focused on assessing the scale and scope of the incident, as well as providing technical mitigation measures.

The UCG remains focused on ensuring that victims are identified and able to remediate their systems, and that evidence is preserved and collected. Additional information, including indicators of compromise, will be made public as they become available.

For additional resources please see:

- CISA suspicious activity detection tool: https://github.com/cisagov/Sparrow
- 12/22 FBI Private Industry Notification
- CISA Insights: What Every Leader Needs to Know About the Ongoing APT Cyber Activity
- CISA Alert: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- NSA Cybersecurity Advisory: Malicious Actors Abuse Authentication Mechanisms to Access Cloud Resources
- December 16, 2020 Joint UCG Statement

###
