Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

SolarWinds Attack—No Easy Fix

Updated December 22, 2020

On December 13, 2020, the cybersecurity firm FireEye published research that a malicious actor was exploiting a supply chain vulnerability in SolarWinds products to hack into government and private sector information technology (IT) networks. SolarWinds confirmed the security incident. The Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive requiring federal agencies to remove certain SolarWinds products from agency networks.

Media initially reported that the U.S. Treasury and Commerce departments were susceptible to this attack; subsequent reports added additional agencies. The list of compromised agencies and companies is expected to expand.

As private sector and government researchers continue investigating this incident, the cybersecurity community expects to learn more about the attack, the adversary, their targets, compromised data and systems, and ways to recover from the incident. This Insight provides an overview of the incident, federal actions, and policy considerations.

The Attack

SolarWinds (Austin, TX) makes IT management products for business customers. These products allow chief information officers (CIOs) to automate certain activities such as managing internet protocol (IP) addresses, monitoring devices, and deploying updates.

A critical element to any software application or platform is the mechanism by which the vendor pushes updates and patches to users. SolarWinds built functions into their products which push update files to users (as is common practice).

A malicious actor discovered a way to compromise SolarWinds' software update service for the Orion IT management platform (a SolarWinds suite of products). The actor was able to compromise the update channel used by Orion to distribute malware. When run, the code executed the Sunburst malware in the SolarWinds IT management platform. Once executed, Sunburst would go dormant for a period of time (to avoid detection) before fetching additional instructions from its command-and-control (C2) server. The additional instructions allowed the actors to exfiltrate files, execute new commands, profile the system, and manipulate machines. The actors sought to hide their presence by manipulating files and disguising their activity as normal network traffic. SolarWinds stated that of their 300,000-plus customers, roughly

Congressional Research Service
https://crsreports.congress.gov
IN11559

18,000 are susceptible to this attack. Known vulnerable versions of the platform were released in spring 2020 and were still vulnerable through mid-December 2020.

The attack is likely part of a larger campaign to which there is no easy fix. The malware allowed the malicious actors a foothold in their victims' networks. From there, they could persist in the network through the creation of additional credentials for other software platforms. So merely remedying the vulnerable versions of SolarWinds' products would be insufficient in eradicating the unauthorized actors from compromised networks.

News media and government officials have attributed the attack to Russia, but the Russian government has denied involvement and a federal agency has yet to confirm attribution. The National Security Agency (NSA) recently attributed another exploit to VMWare products to Russian state-sponsored actors and said both vulnerabilities can be used in conjunction.

FireEye previously disclosed a breach of its own hacking tools. FireEye's breach did not contain unknown exploits or techniques, so the SolarWinds vulnerability was not part of that breach.

Federal Actions

CISA directed federal agencies to remove and disable certain SolarWinds products and start hunting for adversaries on their networks, while remaining wary that the adversary may be able to observe any remediation action an organization takes.

CISA guidance encourages agencies with resident expertise to investigate for new accounts and network traffic for new domains. If an agency does not have this expertise, they may request technical assistance from CISA. While these actions are compulsory for federal agencies, CISA recommends nonfederal entities also undertake these actions.

CISA promised to continue working with federal and nonfederal partners to discover more information about this exploitation and is to provide additional guidance and remediation actions when available. For example, CISA subsequently amended their guidance to include guidance for cloud computing environments.

The National Security Council has activated the National Cyber Incident Response Plan and has stood up the Unified Coordination Group to streamline interagency collaboration.

The National Counterintelligence and Security Center warned of software supply chain attacks in 2019. The Defense Science Board warned of software update risks in 2017.

Policy Considerations

Cybersecurity is not a static goal. Instead, it is a risk management process, which involves continual work. The National Institute of Standards and Technology (NIST) *Cybersecurity Framework* categorizes this process cycle as: (1) identify; (2) protect; (3) detect; (4) respond; and (5) recover. Much of the recent cybersecurity policy work has been on the first three processes; the SolarWinds attack highlights the need for the last two.

Given the nature of the SolarWinds attack, it is unlikely existing programs would have prevented this incident. The Federal Information Security Modernization Act (FISMA) lays out roles for federal agency cybersecurity, but ultimately places implementation responsibility with agency heads. Other recent congressional activities, such as the SECURE IT Act and the IT MGT Act, address how agencies acquire and deploy technology, but not how to manage it once it's deployed. Agencies were recently directed to create vulnerability disclosure programs (VDPs), but government contractors were not required to have a VDP.

Incident response capabilities may be over-taxed in the aftermath of this incident. The nature of the attack granted the malicious actors great latitude to move about networks and carry out their objectives. Agencies and private sector companies may lack the expertise or capacity to conduct hunt activities on their own networks. Additionally, third party IT companies may not have the requisite experience in:

- addressing advanced persistent threats on networks; and
- dealing with organizations of different sizes, complexity, and operations.

This may create a delay in remediating the consequences of the attack.

Addressing the response provides policymakers opportunities to dictate subsequent federal actions to victim companies, agencies, and attributed perpetrators, and could inform how the private sector will prioritize scarce resources. Lessons learned from this attack may also inform systemic changes to cybersecurity policy. Office of Management and Budget (OMB) guidance requires agencies to plan for incident response activities, but does not specifically address this particular risk.

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer