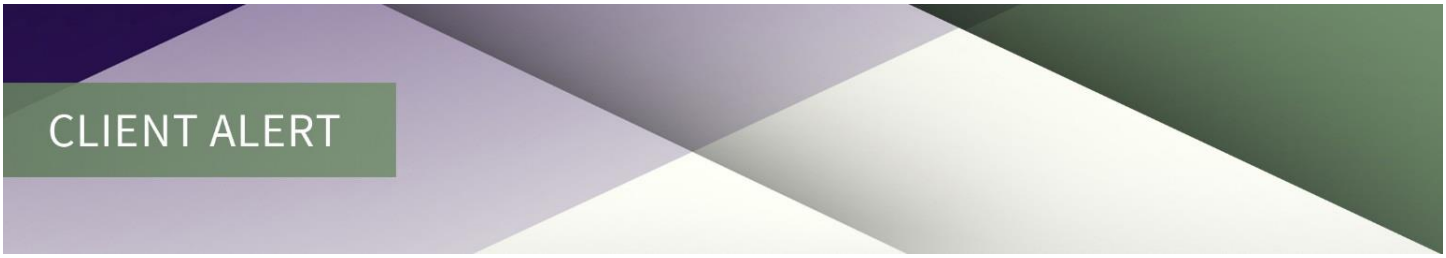
WILLKIE FARR & GALLAGHER LLP



U.S. Government Organizations, Critical Infrastructure Entities, and Private Sector Organizations Face "Grave" Risks From Highly Sophisticated Cyber-Intrusion Campaign

Update to *Client Alert - CISA Issues Emergency Directive to Federal Agencies to Mitigate Compromise of SolarWinds Orion Platform*, Dec. 16, 2020

December 21, 2020

AUTHORS

Elizabeth P. Gray | Elizabeth Bower | Daniel K. Alvarez | Michael J. Gottlieb
Richard M. Borden | Philip F. DiSanto

On December 16, 2020, we released a client alert concerning a significant cybersecurity incident involving the SolarWinds Orion Platform. At that time, the Cybersecurity and Infrastructure Security Agency (CISA) emphasized that the scope of the incident was still under investigation and that potentially affected organizations should take immediate measures to mitigate risks associated with the SolarWinds vulnerability. Since then, law enforcement authorities, security researchers, and news media have disclosed that the SolarWinds incident appears to be part of a broader, ongoing, and highly sophisticated campaign against U.S. government organizations, critical infrastructure entities, and private sector organizations.

In light of the ongoing and evolving nature of this incident, all private sector and non-profit organizations, including those without potential exposure to the SolarWinds vulnerability, should consider taking appropriate technical and legal measures in response. These include (i) assessing data security protections and obligations under contractual provisions

and policies, including with respect to the supply chain, (ii) updating comprehensive cybersecurity programs and incident response plans, (iii) understanding applicable regulatory and disclosure obligations, and (iv) analyzing the potential risk of regulator inquiries, government enforcement actions, and civil litigation.

Recent Efforts to Mitigate the SolarWinds Orion Vulnerability

SolarWinds, FireEye, and Microsoft have reportedly taken measures to mitigate further risks from the SolarWinds Orion Platform vulnerability, including by releasing software patches and known indicators of compromise. Further, FireEye, Microsoft, and GoDaddy have reportedly collaborated to seize control of a malicious domain used by the threat actor in connection with the SolarWinds compromise. While those measures are likely to mitigate further exploitation of the initial SolarWinds vulnerability, organizations that have already been compromised through that vulnerability will need to undertake immediate and long-term measures to identify damage to and persistence mechanisms deployed on their networks.

CISA and security researchers have repeatedly emphasized that detecting and eradicating this particular threat actor from an affected network is likely to be extremely complex, challenging, time-consuming, and costly. Potentially affected organizations should therefore continue to investigate whether and to what extent they were compromised, as the results of such investigations will necessarily inform next steps to remediate identified weaknesses.

Investigation of Additional Initial Access Vectors

On December 17, 2020, CISA also disclosed that it is investigating additional initial access vectors other than the SolarWinds Orion compromise. CISA has continued to release additional information as it becomes available, including that it is investigating incidents in which the same threat actor appears to be abusing tokens for authentication purposes (i.e., "SAML" tokens used for single sign on (SSO) federated identity) on systems where affected SolarWinds instances have not been identified. Moreover, CISA has updated its original alert to emphasize that (i) the threat actor is highly sophisticated, well-resourced, and able to endure on victim networks for extended periods of time, (ii) not all compromised organizations have been subjected to follow-on attacks, and (iii) potentially affected organizations must be highly aware of operational security and their incident response and remediation plans. CISA has also re-emphasized the gravity of the ongoing threat, noting that these cyberattacks pose a "grave risk" to potentially affected organizations, including private sector organizations.

Supplemental Guidance to Affected Organization

On December 18, 2020, CISA also released supplemental guidance reiterating that organizations affected by the SolarWinds vulnerability should not attempt to re-build and re-connect affected systems until further notice, should take measures to avoid re-introducing malicious code through networks, and should continue to perform forensic analyses and searches based on capabilities. In addition, CISA advised agencies to coordinate with any third-party service providers,

such as cloud service providers hosting agency data, and to supplement their incident reporting to CISA with "relevant information" from those third-party service providers.

Analyzing Potential Legal and Regulatory Issues

Private sector and non-profit organizations face significant uncertainty concerning their applicable legal obligations due to the unprecedented scope and complexity of this cybersecurity incident. In particular, public companies and highly regulated organizations that either (i) downloaded the compromised SolarWinds Orion software or (ii) have identified other indicators of compromise on their networks face significant near-term decisions about their disclosure obligations and cooperation with law enforcement. Because CISA has already indicated that the scope of this incident extends beyond SolarWinds and is ongoing, regulators will expect that corporate boards and senior management understand both the technical challenge of responding to this evolving incident, as well as their organizations' legal and regulatory obligations as new information emerges.

* * *

December 16, 2020 Client Alert:

CISA Issues Emergency Directive to Federal Agencies to Mitigate Compromise of SolarWinds Orion Platform

On December 13, 2020, SolarWinds Corporation, a U.S. software company whose products are widely used to manage IT networks, systems, and infrastructure, disclosed that a targeted cyberattack had inserted a vulnerability into certain versions of its Orion centralized IT monitoring and management software. SolarWinds reports providing its products and services to "more than 300,000 customers worldwide," including hundreds of Fortune 500 companies, the top ten U.S. telecommunications providers, the top five U.S. accounting firms, hundreds of universities and colleges, all branches of the United States military, the NSA, the Department of Justice, and the Executive Office of the President of the United States. SolarWinds disclosed in a December 14 SEC filing that it currently believes up to 18,000 of those customers are running the compromised software.

According to FireEye, which reportedly discovered the incident while investigating a related cybersecurity incident that compromised its own systems the week before, the SolarWinds vulnerability is part of a widespread, ongoing campaign by a "highly skilled actor . . . with significant operational security" to gain "access to numerous public and private organizations around the world . . . via trojanized updates to SolarWind's Orion IT monitoring and management software." FireEye also notes that the threat actor responsible for the vulnerability is taking sophisticated measures to avoid detection and maintain its foothold within compromised networks.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an emergency directive to all federal agencies to immediately disconnect devices affected by the SolarWinds vulnerability due to the ongoing nature of the

threat to federal networks, the high potential for the vulnerability to compromise federal agency systems, and the "[g]rave impact of a successful compromise."

The CISA directive requires that all federal agencies take the following measures until further notice:[1]

1. Forensically image all systems hosting the compromised SolarWinds Orion Platform versions, analyze new user or service accounts on those systems, and analyze stored network traffic for indications of compromise, if the agency has the expertise to undertake such measures;

2. Disconnect from the network or power down all systems hosting affected SolarWinds Orion Platform versions and prevent those systems from re-joining the agency's enterprise domain;

3. Block all traffic to and from external hosts on which any version of the SolarWinds Orion Platform has been installed;

4. Identify and remove all accounts controlled by the threat actor and its "identified persistence mechanisms";

5. Report the existence of specific threat-actor installed DLL files or other indications of compromise to CISA as an incident;

6. After removing all threat actor-controlled accounts and identified persistence mechanisms, take measures to rebuild host systems, reset credentials associated with SolarWinds' Orion Platform, and take additional technical measures to eradicate the threat actor from the agency's systems and network; and

7. Submit a template report to CISA attesting that affected devices were disconnected or powered down.

While the CISA directive applies only to federal agencies, the CISA, SolarWinds, and FireEye releases outline immediate measures that organizations in the private sector and non-profit organizations, such as universities and healthcare systems, can take to mitigate the threat posed by the SolarWinds vulnerability. It is anticipated that regulators will rapidly begin asking about implementation of remediation measures.

In addition to implementing publicly available measures to mitigate the impact of this vulnerability, private sector and non-profit organizations should begin to assess and take measures to comply with applicable legal obligations. In particular, organizations should analyze and consider their potential obligations under existing contractual agreements, insurance policies, data protection and privacy laws and regulations (especially safety and soundness requirements), breach

[1] SolarWinds has released a preliminary hotfix to secure its Orion Platform and was in the process of releasing a second hotfix at the time of writing, but CISA's directive instructs federal agencies to "expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available."

notification statutes, and public disclosure laws and regulations. As other high-profile cybersecurity incidents have shown, failing to follow risk management plans, implement incident response plans, respond promptly to publicly reported vulnerabilities, or apply patches and measures designed to mitigate those vulnerabilities, can cause unnecessary harm to third parties and consequently result in civil litigation, regulatory actions involving hefty fines, and other costly government investigations and enforcement actions.

We are monitoring these developments and are available to help you assess the specific issues that your organization may face as a result of this incident.

In addition to implementing publicly available measures to mitigate the impact of this vulnerability, private sector and non-profit organizations should begin to assess and take measures to comply with applicable legal obligations. In particular, organizations should analyze and consider their potential obligations under existing contractual agreements, insurance policies, data protection and privacy laws and regulations (especially safety and soundness requirements), breach notification statutes, and public disclosure laws and regulations. As other high-profile cybersecurity incidents have shown, failing to follow risk management plans, implement incident response plans, respond promptly to publicly reported vulnerabilities, or apply patches and measures designed to mitigate those vulnerabilities, can cause unnecessary harm to third parties and consequently result in civil litigation, regulatory actions involving hefty fines, and other costly government investigations and enforcement actions.

We are monitoring these developments and are available to help you assess the specific issues that your organization may face as a result of this incident.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Michael J. Gottlieb
202 303 1442
mgottlieb@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Philip F. DiSanto
212 728 8534
pdisanto@willkie.com