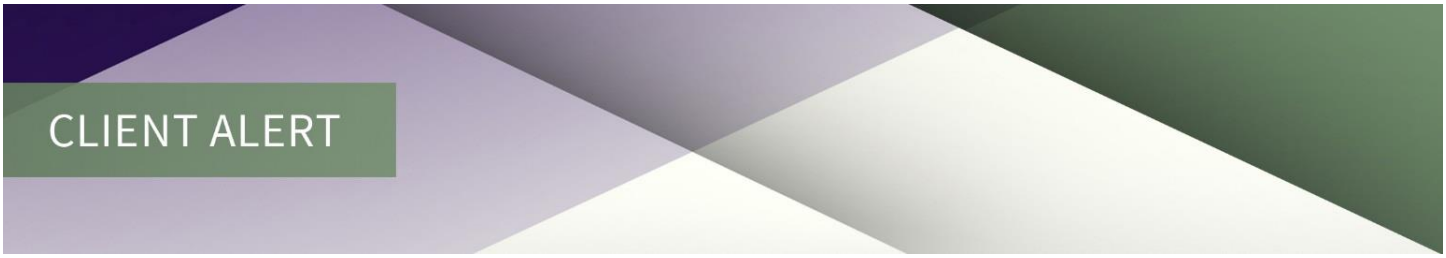

CISA Issues Emergency Directive to Federal Agencies to Mitigate Compromise of SolarWinds Orion Platform

December 16, 2020

AUTHORS

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

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.

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

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.

[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."

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