LEWIS ROCA

URGENT: WIDESPREAD HACKING CAMPAIGN COULD REQUIRE IMMEDIATE ACTION

12/15/2020

FireEye, Inc., a leading U.S. cybersecurity firm, recently disclosed that it had been hacked by a nation-state actor. The company has since revealed that the hack was likely perpetrated, in part, through an ***ongoing compromise*** of "Orion" IT monitoring and management software offered by SolarWinds Worldwide, LLC.

Additional reports indicate that the U.S. Department of the Treasury and other agencies have also been affected by the breach, and thousands of other entities could be involved, as SolarWinds boasts more than 300,000 customers, including more than 425 of the Fortune 500, all of the top-ten U.S. telecom companies, all five branches of the U.S. military, and all of the top-five U.S. accounting firms. Indeed, according to FireEye, the hacking campaign resulting from the SolarWinds compromise is widespread and has likely affected numerous public and private organizations around the world.

As a result of this news, the U.S. Cybersecurity & Infrastructure Agency (CISA) has issued an ***emergency directive*** to all federal civilian executive branch agencies. The directive indicates that the SolarWinds exploit "poses an unacceptable risk" to the agencies and "requires emergency action," including the immediate disconnection or powering down of Orion products and the blocking of all traffic to and from external hosts with any version of Orion software installed. Although the CISA directive applies only to federal agencies, almost every organization (including state agencies, for-profit companies, and non-profits) should take note of the advice contained in the directive and take immediate action to address the issue.

We encourage you to confer ***as soon as possible*** with your information-technology personnel to determine if your organization might have been affected by this incident. If your organization was or might have been affected by this incident, you might want to consider taking immediate steps similar to those outlined in the CISA directive. In addition, please feel free to contact a member of our Data Protection and Cybersecurity Team if you would like to discuss this incident or if you have any other questions pertaining to data privacy or security.

Professionals

- John C. Gray, CIPP/US

Practice Areas

- Data Privacy and Cybersecurity

Offices

- Phoenix

Region

- Arizona