# SolarWinds hack

PARTNER UPDATE – January 26th, 2021

Dear KIS Clients,

We have all heard by now a lot about the SolarWinds hack and the impact on a number of partners such as FireEye and others. The impact to the client community has crossed sectors from corporate to government as well as healthcare and many others. Any organization that has SolarWinds deployed is likely to be at risk and should go through (or must go through if government) the CISA remediation in accordance with their remediation directive (Emergency Directive 21-01) and updates as they become available.

We continue to monitor the situation and are seeing more and more details come forward that appear to broaden the overall impact. Last week, we noticed that the Raindrop malware (found as another part of the attack) is distributing cobalt strike (a red team tool that bad actors can use to compromise your environment). We also saw that Malwarebytes was added to the list of companies hit by the same hackers and SonicWall also reported a similar breach that impacted a few of their products. Most security watchdogs say this isn't over yet and to keep an eye out.

KIS can help ease concerns with the above by reviewing your defenses and recommending changes to your cybersecurity program that will directly reduce your exposure to these and many other threats. Whether you use any of the tools listed or the next ones that get announced, following a checked and reviewed model by qualified security professionals is a practice that any security-aware organization should perform. We at KIS are here to help, and we would like to work with you.

Sincerely,

Craig

**Craig Miller**
Director of Infrastructure & Security Practices
KIS - Keep IT Simple | Professional IT Solutions Experts Since 1988
E: miller@kiscc.com
O: (510) 403-7500