NCSC statement on the SolarWinds compromise

The latest statement from the NCSC following the reported SolarWinds compromise.

Paul Chichester, NCSC Director of Operations, said:

“This is a complex, global cyber incident, and we are working with international partners to fully understand its scale and any UK impact.

“That work is ongoing and will take some time, but simply having SolarWinds does not automatically make an organisation vulnerable to real world impact.

“The NCSC is working to mitigate any potential risk, and actionable guidance has been published to our website. We urge organisations to take immediate steps to protect their networks - and will continue to update as we learn more.”

Further information

- Read the NCSC’s guidance for SolarWinds’ Orion suite customers. Enhanced technical guidance is available on the NCSC's Cyber Security Information Sharing Partnership (CiSP) platform.
- We recommend that organisations ensure any affected instances of SolarWinds Orion are installed behind firewalls disabling internet access (both outbound and inbound) for the instances.
- SolarWinds customers will only be vulnerable if a number of extra variables are in place.
- FireEye has published a blog updating on its investigation. We recommend that organisations read the blog and follow the suggested mitigations where relevant.

- Microsoft has published a blog outlining the steps that government and the private sector can take to protect themselves from this kind of cyber attack.
- The NCSC has previously published guidance on how to develop and implement a secure system administration strategy.

PUBLISHED

21 December 2020

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

NEWS TYPE

Statement