Dealing with the SolarWinds Orion compromise

Immediate actions for all organisations using the SolarWinds Orion suite of IT management tools

> **Last updated**
> This page was last updated at 11:30 on 08 January 2021.
>
> Enhanced technical guidance is available on the NCSC's Cyber Security Information Sharing Partnership (CiSP) platform.

SolarWinds Orion, the popular IT system management platform, has been compromised and may be used for onward attacks against systems connected to the product.

An attacker has been able to add a malicious, unauthorised modification to SolarWinds Orion products which allows them to send administrator-level commands to any affected installation. This modification:

- causes the Orion products to connect to an attacker-controlled server to request instructions
- does **not** rely on the attacker being able to directly connect from the internet to the Orion server

There is evidence of the attacker using this capability in some cases to move from a single Orion server to other parts of the victim's IT network.

Not all customers who have an installation with the unauthorised, malicious modification will have been seriously affected, but all should take immediate action.

This guidance is liable to change as further information becomes available. If you discover you have a compromised system please check back for updates.

Who this advice is for

All users of the SolarWinds Orion suite of network and IT management tools should implement the following steps immediately.

These steps should be carried out by technical staff who have experience of the *SolarWinds Orion* package.

Find out if you have an affected system

1. Identify if you have a product from the *SolarWinds Orion* suite versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1. *SolarWinds Orion* suite consists of several products; for exact products see the SolarWinds advisory.
2. If you are able to, check any internet web proxy, DNS proxy, or firewall logs for connections to the legitimate Solarwinds update site of downloads.solarwinds.com. This may help in identifying possible Orion Suite products. (Note, this will likely identify any *SolarWinds* products, not just the Orion Suite).
3. If you find any *Orion Suite* products on your network, then check for a file named **SolarWinds.Orion.Core.BusinessLayer.dll**, and generate a SHA-256 hash of the file. You can use the Powershell command Get-FileHash to do this. Upload this hash to VirusTotal and check if it is detected as malicious. If it is detected then you have a copy of SolarWinds that has maliciously added functionality. This DLL is referred to as SUNBURST by FireEye.
4. Check any internet web proxy, DNS proxy or firewall logs for connections to any sub-domain of avsvmcloud[.]com (which is used for command and control by the initial backdoor).
5. FireEye have released multiple technical detection rules for the malicious DLL (which they call SUNBURST). If you have the ability to run these checks, then you should do so.

Actions to take immediately if you have an affected system

1. If you find that you have a version of *SolarWinds Orion suite* versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1, then an attacker may have backdoored this software and you should isolate the server from the internet immediately.
2. After you have isolated your server from the internet, if your affected system has the SUNBURST DLL file listed above, and if you were able to resolve api.solarwinds.com from the host prior to locking down access (and *especially* if you have evidence of queries to avsvmcloud[.]com), then unknown, malicious software has been executed on your server and you should act accordingly (see 'In all cases' below). If your host has the SUNBURST DLL, but did **not** have the ability to resolve api.solarwinds.com, then although you had the malicious software on your system, your defence-in-depth controls have stopped the malicious software from connecting to its control server. You should however update to a known-good version of your Orion product (see the SolarWinds advisory for details).
3. Due to the ongoing nature of investigations into this incident, the NCSC has limited information on the actions that an attacker may have performed on affected systems. One known route is deploying a payload referred to as TEARDROP. You can check for evidence of TEARDROP on the affected device by looking for a file named "C:\WINDOWS\SysWOW64\netsetupsvc.dll".
4. If the file "*C:|WINDOWS|SysWOW64|netsetupsvc.dll*" is present in the specified location on your server, please contact the NCSC immediately, via https://report.ncsc.gov.uk/ for further assistance.

In all cases

1. Any hosts which have, at any time, had one of the affected versions of *SolarWinds Orion* installed, may have been compromised. If you find the DLL

and/or DNS queries listed above then your system has definitely executed unknown attacker originated code. Organisations should follow their own processes for dealing with a suspected server compromise.

2. Consider measures such as:

- Resetting any credentials which the server has had access to
- Identifying any anomalous behaviour that the server, or accounts that have logged into the server, may have performed
- Investigating any other suspicious activity. In particular, look for remote logins by legitimate accounts, originating from IP addresses that belong to virtual server hosting services.

3. Once you have investigated, you should definitely update your affected products in line with SolarWinds advice. You may wish to consider a full rebuild of the *SolarWinds* host as part of your remediation.

Getting help

If you are not able to deal with a suspected server compromise of this nature, you should contact an NCSC-listed Cyber Incident Response company.

More information

- *SolarWinds* have published a security advisory on this incident. This includes details of affected software and the vendor's advice on resolving the specific issue of the malicious modification of their software. However, any affected organisation should also perform a thorough search for any evidence of further compromise, in addition to taking the steps outlined in this advisory.

- FireEye, who discovered the compromise, has published a blog on its investigation. This includes extensive technical details which may help in investigation of a suspected server compromise.
- Microsoft has published a blog on this attack which includes other potential routes for investigation of compromise.
- Enhanced technical guidance is available on the NCSC's Cyber Security Information Sharing Partnership (CiSP) platform.
- The NCSC has previously published guidance on how to develop and implement a secure systems administration strategy.

PUBLISHED

15 December 2020

REVIEWED

21 December 2020

VERSION

2.0

WRITTEN FOR

Public sector

Small & medium sized organisations

Large organisations

Cyber security professionals