## Security Advisory 2020-060

# Multiple Vulnerabilities in SolarWinds Orion

*January 12, 2021 — v1.2*

**TLP:WHITE**

*History*

- *16/12/2020 — v1.0 – Initial publication*
- *22/12/2020 — v1.1 – Version updated with additional technical information*
- *11/01/2021 — v1.2 – Version updated with additional information*

## Summary

Multiple vulnerabilities have been discovered in **SolarWinds Orion**, a popular Network Management System software, the most severe of which could allow for arbitrary code execution [2, 3]. Numerous public and private organisations around the world are affected. Additionally, the attackers gained access to victims via *trojanised* SolarWinds Orion updates [1, 4, 5]. The attack was a very sophisticated supply chain attack. In this case, it appears that the code was intended to be used in a targeted way as its exploitation requires manual intervention. The campaign has been dubbed **SunBurst** by FireEye and **Solarigate** by Microsoft.

While the malicious activity was only made public in *December 2020*, researchers at *ReversingLabs* analysed **SolarWinds** binaries and identified modifications to installer packages as early as *October 2019* [6].

While analyzing artifacts from the **SolarWinds Orion** supply-chain attack, another backdoor has been discovered, named **Supernova**. The malware is a webshell planted in the code of the Orion network and applications monitoring platform and enabled adversaries to run arbitrary code on machines running the *trojanised* version of the software. This had been thought to be part of the intrusion toolset but in reality this was a different piece of malware, targeting **SolarWinds Orion** installations that had been left unpatched for a vulnerability tracked as **CVE-2019-8917** and exposed online. [11, 13, 14]

## Technical Details

Details of these vulnerabilities are as follows:

- A security vulnerability due to the possibility to define an arbitrary Visual Basic script **(CVE-2020-14005)** [2]
- An HTML injection vulnerability **(CVE-2020-13169)** [3]
- A Network Performance Monitor vulnerability **(CVE-2019-8917)** [12]

### SunBurst/Solarigate

Additionally, as part of the campaign known as **SunBurst** (FireEye) or **Solarigate** (Microsoft), the attackers inserted malicious code into `SolarWinds.Orion.Core.BusinessLayer.dll`, a code library belonging to the SolarWinds Orion Platform. The code was injected in a method that gets invoked periodically, ensuring both execution and persistence, so that the malicious code is always guaranteed to be up and running - a method named `RefreshInternal` was used [8]. The DLL was then distributed to SolarWinds customers in a supply chain attack leveraging the update mechanism of Orion.

This DLL backdoor is loaded by the `SolarWinds.BusinessLayerHost.exe` program. Once loaded, it will connect back to the remote Command & Control server at a subdomain of `avsvmcloud[.]com` to receive *tasks* to execute on the infected computer.

Observing a CNAME response from a DNS query to `avsvmcloud[.]com` is the best way to determine if your organisation was of interest to the threat actor and potentially the victim of a much more serious breach [9].

The backdoor goes through an extensive list of checks to make sure it is running in an actual enterprise network and not on an analyst's environment:

- It verifies that the process hosting the malicious DLL is named `solarwinds.businesslayerhost.exe`.
- It checks that the last write-time of the malicious DLL is at least 12 to 14 days earlier.
- It delays execution by random amounts of time.
- It verifies that the domain name of the current device meets the following conditions:
  - The domain must not contain certain strings; the check for these strings is implemented via hashes, so at this time the domain names that are block-listed are unknown.
  - The domain must not contain `solarwinds`.
  - The domain must not match the regular expression `(?i)([^a-z]|^)(test)([^a-z]|$)`.
- It checks that there are no running processes related to security-related software.
- It checks that there are no drivers loaded from security-related software.
- It checks that the status of certain services belonging to security-related software meets certain conditions.
- It checks that the host `api.solarwinds.com` resolves to an expected IP address.

In its first step, the backdoor initiates a connection to a predefined C2 server to report some basic information about the compromised system and receive the first commands. The C2 domain is composed of four different parts: three come from strings that are hardcoded in the backdoor, and one component is generated dynamically based on some unique information extracted from the device. This means that every affected device generates a different subdomain to contact.

The dynamically generated portion of the domain is computed by hashing the following data:

- the physical address of the network interface,

- the domain name of the device,

- the content of the `MachineGuid` registry value from the key:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
  ```

The backdoor also generates a pseudo-random URI that is requested on the C2 domain. Like the domain, the URI is composed using a set of hardcoded keywords and paths, which are chosen partly randomly and partly based on the type of HTTP request that is being sent out.

Finally, the backdoor composes a JSON document into which it adds the unique user ID, a session ID, and a set of other non-relevant data fields. It then sends this JSON document to the C2 server.

Once operating inside a network, threat actors can perform reconnaissance on the network, elevate privileges, and move laterally. Attackers progressively move across the network until they can achieve their goals [8, 10].

### Supernova

Based on investigations related to **Supernova** [4]:

- **Supernova** is not malicious code embedded within the builds of **SolarWinds Orion Platform** as a supply chain attack. It is malware that is separately placed on a server that requires unauthorised access to a customer's network and is designed to appear to be part of a **SolarWinds** product.
- The **Supernova** malware consisted of two components. The first was a malicious, unsigned webshell DLL `app_web_logoimagehandler.ashx.b6031896.dll` specifically written to be used on the **SolarWinds Orion Platform**. The second is the utilisation of a vulnerability in the **Orion Platform** to enable deployment of the malicious code. This vulnerability in the **Orion Platform** has been resolved with the latest updates.

## Products Affected by SunBurst

**SolarWinds Orion Platform** versions affected by **SunBurst**: **2019.4 HF 5**, **2020.2 with no hotfix installed** and **2020.2 HF 1**, including [11]:

- Application Centric Monitor (ACM)
- Database Performance Analyzer
- Integration Module (DPAIM)
- Enterprise Operations Console (EOC)
- High Availability (HA)
- IP Address Manager (IPAM)
- Log Analyzer (LA)
- Network Automation Manager (NAM)
- Network Configuration Manager (NCM)
- Network Operations Manager (NOM)
- User Device Tracker (UDT)
- Network Performance Monitor (NPM)
- NetFlow Traffic Analyzer (NTA)
- Server & Application Monitor (SAM)
- Server Configuration Monitor (SCM)
- Storage Resource Monitor (SRM)
- Virtualization Manager (VMAN)
- VoIP & Network Quality Manager (VNQM)
- Web Performance Monitor (WPM)

While the investigations are ongoing, **SolarWinds** states that they are not aware that this **SunBurst** vulnerability affects other versions of **Orion Platform** products. They are also investigating their non-Orion products, but for the moment there is no evidence to have been impacted by the **SunBurst** vulnerability.

## Products Affected by Supernova

**SolarWinds Orion Platform** versions affected by **Supernova**:

- 2020.2.1 HF1
- 2020.2.1
- 2020.2 HF1
- 2020.2
- 2019.4 HF5
- 2019.4 HF4
- 2019.4 HF3
- 2019.4 HF2
- 2019.4 HF1
- 2019.4
- 2019.2 HF3
- 2019.2 HF2
- 2019.2 HF1
- 2019.2
- 2018.4
- 2018.2

as well ass all the prior versions.

## Recommendations

**SolarWinds** has released software updates that address the vulnerabilities described in this advisory [4].

CERT-EU recommends the following:

### For SunBurst

- Those who do not have the identified malicious binary:
  - To patch their systems and resume using them as determined by and consistent with their internal risk evaluation.
- Those who have identified the presence of the malicious binary - with or without beaconing to `avsvmcloud[.]com`:
  - Owners with the identified malicious binary whose vulnerable applications' only unexplained external communications are with `avsvmcloud[.]com` — a fact that can be verified by comprehensive network monitoring — can harden the device, re-install the updated software from a verified supply chain, and resume use as determined by and consistent with a thorough risk evaluation.
- Those with the binary beaconing to `avsvmcloud[.]com` and secondary C2 activity to a separate domain or IP address"
  - If you observed communications with `avsvmcloud[.]com` that appear to suddenly cease prior to 14 December 2020 — not due to an action taken by your network defenders - assume the environment has been compromised, and initiate incident response procedures immediately [7].

### For Supernova

Check for access to URI: `logoimagehandler.ashx` in your logs. If any ingress traffic to `logoimagehandler.ashx` is observed, with a combination of `codes, clazz, method or args` parameters in any order of the query string are strong indicators of compromise (IOCs). If a detection fires on this combination in any order, please isolate and image your Orion instance immediately. If the request came internal to the network, then it is highly probable that the user that initiated the request has also been compromised. IOCs from https://unit42.paloaltonetworks.com/solarstorm-supernova/ can be used to detect potential compromise.

## References

[1] https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-solarwinds-orion-could-allow-for-arbitrary-code-execution_2020-166/

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14005

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13169

[4] https://www.solarwinds.com/securityadvisory

[5] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[6] https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident#

[7] https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[8] https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

[9] https://www.volexity.com/blog/2020/12/16/responding-to-the-solarwinds-breach/

[10] https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

[11] https://www.bleepingcomputer.com/news/security/new-supernova-backdoor-found-in-solarwinds-cyberattack-analysis/

[12] https://support.solarwinds.com/SuccessCenter/s/article/CVE-2019-8917-NPM-Vulnerability?language=en_US

[13] https://twitter.com/ItsReallyNick/status/1339530685548290051?s=20

[14] https://unit42.paloaltonetworks.com/solarstorm-supernova/