

## SolarWinds Orion Attack

### The SolarWinds supply chain attack

<https://www.solarwinds.com/securityadvisory>  
 CVEs: CVE-2020-10148

SolarWinds [signed] software containing a planted vulnerability released in March 2020 as a regular (trusted) software patch. The backdoor was not discovered until the FireEye breach became public 9 months later.

**Background** SolarWinds was the victim of a complex & targeted supply chain cyber attack, with the primary goal of inserting a malicious backdoor into trusted (signed) software, which could later be exploited in end-customer installations of the SolarWinds Orion platform. As reported by SolarWinds, the earliest visible account of the attacker shows test code inserted in the October, 2019 software release.  
<https://www.solarwinds.com/securityadvisory>

It's been claimed the attackers first gained access to SolarWinds infrastructure by exploiting an Authentication Service vulnerability. They were then able to persist and monitor emails & files, to identify the developers they needed to target. Once identified, the targets were infiltrated using Spear Phishing techniques to infect their local compute instances trusted to check-in source code. Starting in March, 2020, SolarWinds began distributing infected patches via its website (as regular software patches) to unsuspecting SolarWinds Orion customers. The impacted versions are 2019.4 HF 5, 2020.2 unpatched, and 2020.2 HF 1. Once upgraded to the vulnerable version, the initial foothold is obtained to the end customer's SolarWinds Development Server, and the malware can then target desired endpoints to install the infiltration malware to those systems. Post-installation to the victim, it may download subsequent malware and eventually make connection to the C&C server. On December 8, 2020, FireEye announced it was the victim of a cyber attack, disclosing that some of its advanced "red team" tools had been stolen. Within the following week, they determined the breach was due to the SolarWinds vulnerability.

**Announced** SolarWinds subsequently released a detailed announcement:  
<https://www.solarwinds.com/securityadvisory#anchor1>

**Latest Developments** On December 13, 2020, CERT issued Emergency Directive 21-01 regarding this issue:  
<https://us-cert.cisa.gov/ncas/alerts/aa20-352a>

## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

Delivery

AV

Blocks trojan payload

 FortiGate DB 84.548	 FortiWeb DB 84.548	 FortiClient DB 84.548	 FortiSASE DB 84.548	 FortiMail DB 84.548	 FortiCASB DB 84.548	 FortiCWP DB 84.548
 FortiADC DB 84.548	 FortiProxy DB 84.548					

App Control

Block/Detect communication to the attack surface (Orion Platform)

FortiGate  
DB 16.989

AV (Pre-filter)

Blocks trojan payload

 FortiSandbox DB 84.548	 FortiNDR DB 84.548
-------------------------------	---------------------------

Exploitation

IPS

Blocks Exploit & lateral movement

 FortiGate DB 16.981	 FortiSASE DB 16.981	 FortiNDR DB 16.981	 FortiProxy DB 16.981
----------------------------	----------------------------	---------------------------	-----------------------------

Installation

C2

Action

## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer  
DB 1.00033

Threat Hunting

 FortiSIEM v5.0+	 FortiEDR
------------------------	--------------

Playbook

FortiSOAR  
v6.4+

## RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

 NSE Training	 Response Readiness
------------------	------------------------

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

## IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

 FortiClient	 FortiEDR
-----------------	--------------

## Additional Resources

- CISA <https://www.cisa.gov/uscert/ncas/alerts/aa20-352a>
- The Hacker News <https://thehackernews.com/2020/12/a-new-solarwinds-flaw-likely-had-let.html>
- Bleeping Computer <https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/>

Learn more about [FortiGuard Outbreak Alerts](#)