SolarWinds

In the Wild since March/2020

https://www.solarwinds.com/securityadvisory

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:

https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

On December 13, 2020, CERT issued Emergency Directive 21-01 regarding this issue:

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

SolarWinds subsequently released a detailed announcement here:

https://www.solarwinds.com/securityadvisory#anchor1

Announced

https://www.solarwinds.com/securityadvisory#anchor1

Latest Developments

https://www.solarwinds.com/sa-overview/securityadvisory#anchor1

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**AV**	*82.548*	Blocks trojan payload
	App Control	*16.981*	Block/Detect communication to the attack surface (Orion Platform)
	IPS	*16.981*	Blocks Exploit & lateral movement
	Web Filter	*SaaS*	Blocks known IOC
	Botnet C&C	*16.981*	Blocks known C&C
FortiClient	**Vulnerability**	*1.229*	Identifies vulnerable host
FortiEDR	**EDR**	*4.0 - 5.0*	Defuses compromised host behaviours & callbacks (zero day protection)
FortiAI	**ANN**	*1.057*	FortiAI detects sample as Backdoor please see FortiAI VSA.
FortiAnalyzer	**IOC**	*0.01727*	Detect IOC / C&C communications
	Event Handlers & Reports	*6.2 - 7.0*	Detects indicators attributed to Solarwinds detections across fabric
FortiSIEM	**IOC**	*0.01727*	Detect IOC / C&C communications
	Rules & Reports	*5.0 - 6.2*	Detects indicators attributed to Solarwinds detections across fabric
FortiSOAR	**Playbook**	*6.4.3*	Playbook for Solarwinds detections
FortiClient/EMS	**Threat Hunting**	*6.2 - 7.0*	Detects vulnerable hosts
	ZTNA Auto Tagging	*6.4 - 7.0*	Auto tagging of vulnerable endporints, can be used in fabric automation

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV
Version Info: 82.548
Link: https://www.fortiguard.com/encyclopedia/virus/8279742/w32-sunburst-a-tr

App Control
Version Info: 16.981
Link: https://www.fortiguard.com/appcontrol/49721

FortiClient
Vulnerability
Version Info: 1.229
Link: https://www.fortiguard.com/updates/epvuln?version=1.229

FortiAI
ANN
Version Info: 1.057
Link: https://filestore.fortinet.com/fortiguard/downloads/FortiAI_Solarwind_846e27a652a5e1bfb0ddd38a16dc865.pdf

Exploitation

FortiGate
IPS
Version Info: 16.981
Link: https://www.fortiguard.com/encyclopedia/ips/49692/solarwinds-sunburst-backdoor

Installation

FortiGate
Web Filter
Version Info: SaaS
Link: https://www.fortiguard.com/webfilter?q=avsvmcloud.com&version=8

C2

FortiEDR
EDR
Version Info: 4.0 - 5.0
Link: https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack

Action

Endpoint

FortiClient/EMS
Threat Hunting
Version Info: 6.2 - 7.0
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD50877

ZTNA Auto Tagging
Version Info: 6.4 - 7.0
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD50882

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
IOC
Version Info: 0.01727
Link: https://ioc.fortiguard.com/search?query=Sunburst&filter=tags

Event Handlers & Reports
Version Info: 6.2 - 7.0
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD50871

FortiSIEM
IOC
Version Info: 0.01727
Link: https://ioc.fortiguard.com/search?query=Sunburst&filter=tags

Rules & Reports
Version Info: 5.0 - 6.2
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51637

FortiSOAR
Playbook
Version Info: 6.4.3
Link: https://fusecommunity.fortinet.com/viewdocument/solarwinds-backdoor-sunburst-inci