# **SolarWinds Orion Supply Chain Attack (2020)**

### **1. Core Issue**

The SolarWinds incident was fundamentally a **supply chain compromise**. Attackers infiltrated SolarWinds’ software build environment and inserted malicious code (SUNBURST) into Orion updates. Since these updates were digitally signed and distributed via official channels, customers trusted them. The flaw was not in the Orion product itself but in the **integrity of the software build and distribution pipeline**, showing that traditional defenses like code signing are insufficient when the build process itself is compromised.

### **2. Who Was Attacked**

The primary target was **SolarWinds**, a Texas-based IT management company. The attackers gained access to its internal development systems and tampered with software builds. The real goal, however, was not SolarWinds alone but its **customers**, which included sensitive organizations worldwide.

### **3. Who Was Affected**

An estimated **18,000 organizations** installed the Trojanized Orion updates. Victims included:

* U.S. federal agencies (Department of Homeland Security, Treasury, Commerce).
* Fortune 500 companies across tech, finance, and healthcare.
* Critical infrastructure providers and research institutions.  
   Not every installation was actively exploited, but the attackers handpicked high-value targets for **follow-on intrusions**.

### 

### **4. Exploit Chain Details**

The attack unfolded in several stages:

1. **Initial Compromise** – Threat actors accessed SolarWinds’ development environment.
2. **Insertion of Malicious Code** – A backdoor (SUNBURST) was added into Orion builds without detection.
3. **Code Signing & Distribution** – Compromised updates were signed with SolarWinds’ certificates and distributed through official update servers.
4. **Deployment in Victim Networks** – Customers installed the updates, unknowingly deploying malware.
5. **Command and Control (C2)** – SUNBURST contacted attacker-controlled servers and awaited instructions.
6. **Selective Exploitation** – Attackers activated secondary payloads only on chosen targets, enabling credential theft, lateral movement, and espionage.

### **5. Prevention / Protection Steps**

* **Secure Build Environments**: Isolate build servers, enforce multi-factor authentication, and apply strict access control.
* **Software Supply Chain Monitoring**: Use build attestation frameworks like SLSA or in-toto to verify build integrity.
* **Zero Trust Principles**: Do not automatically trust vendor updates—validate behavior post-deployment.
* **Telemetry & Monitoring**: Deploy endpoint detection (EDR) and SIEM tools to catch anomalies such as unusual network connections.

### 

### 

### **6. Fixes & Vendor Response**

* SolarWinds released **cleaned versions of Orion** and revoked compromised certificates.
* Customers were advised to patch immediately and rotate credentials.
* Microsoft and other partners released detection signatures for SUNBURST.
* U.S. CISA published detailed **mitigation advisories (AA20-352A)** with steps to detect and remediate infections.

### **7. Reference Material**

* CISA Emergency Directive 21-01 – SolarWinds Orion Compromise:  
   https://www.cisa.gov/news-events/alerts/emergency-directive-21-01
* FireEye (Mandiant) – SolarWinds Supply Chain Compromise Analysis:  
   https://www.mandiant.com/resources/solarwinds-supply-chain-compromise
* Microsoft Security Blog – Solorigate Analysis and Guidance:  
  <https://www.microsoft.com/security/blog/2020/12/13/customer-guidance-related-to-recent-nation-state-cyber-attacks/>
* SolarWinds SEC Filings and Incident Reports:  
   https://investors.solarwinds.com/financial-information/sec-filings
* ENISA Threat Landscape for Supply Chain Attacks (2021):  
   https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
* U.S. Government Accountability Office (GAO) – Lessons from SolarWinds:  
   https://www.gao.gov/products/gao-21-104714

### **8. Further Reading**

* Harvard Belfer Center – “The SolarWinds Hack: A Case Study in Supply Chain Compromise”:  
   https://www.belfercenter.org/publication/solarwinds-hack
* SANS Institute – SolarWinds Lessons Learned Webinar:  
   https://www.sans.org/webcasts/solarwinds-supply-chain-attack-lessons-learned/
* CrowdStrike Global Threat Report 2021 – Case Studies:  
   https://www.crowdstrike.com/global-threat-report/
* NIST Cybersecurity Framework – Supply Chain Risk Management:  
  <https://www.nist.gov/cyberframework/supply-chain>
* OpenSSF Best Practices for Software Supply Chain Security:  
   https://openssf.org/

### **9. Tooling**

* Zeek Network Security Monitor – Detecting C2 activity:  
   https://zeek.org/
* EDR Platforms (e.g., Microsoft Defender for Endpoint, CrowdStrike Falcon):  
   https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/
* SBOM Generators (Syft, CycloneDX) – Identifying affected components:  
  <https://github.com/anchore/syft>
* in-toto & SLSA Provenance Framework – Securing build pipelines:  
   https://in-toto.io/
* YARA Rules and IOC Feeds from CISA & FireEye:  
  <https://github.com/fireeye/sunburst_countermeasures>
* SIEM Correlation Rules for Solorigate TTPs:  
   https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-008a