kindred

Security Newsletter

21 December 2020

Subscribe to this newsletter

SolarWinds: 18,000 Customers installed backdoored software, 40+ victims identified

SolarWinds, the enterprise monitoring software provider which found itself at the epicenter of the most consequential supply chain attacks, said as many as 18,000 of its high-profile customers might have installed a tainted version of its Orion products. The Texas-based company serves more than 300,000 customers worldwide, including every branch of the US military and four-fifths of the Fortune 500 companies.

The company also reiterated in its security advisory that besides 2019.4 HF 5 and 2020.2 versions of SolarWinds Orion Platform, no other versions of the monitoring software or other non-Orion products were impacted by the vulnerability.

Troublingly, according to a report from security researcher Vinoth Kumar, it also appears that a publicly-accessible SolarWinds GitHub repository was leaking FTP credentials of the domain "downloads.solarwinds.com," thus allowing an attacker to potentially upload a malicious

executable disguised as Orion software updates to the downloads portal. Even worse, the FTP server was protected by a trivial password.

The development comes a day after cybersecurity firm FireEye said it identified a nine-month-long global intrusion campaign targeting public and private entities that introduce malicious code into legitimate software updates for SolarWinds' Orion software to break into the companies' networks and install a backdoor called SUNBURST. The US Department of Homeland Security was breached, as were the departments of Commerce and Treasury, Reuters reported yesterday. The espionage campaign also included the December 8 cyberattack on FireEye, although it's not immediately clear whether the intrusion and exfiltration was a direct result of a rogue SolarWinds update.

Microsoft said that over 40 of its customers had their networks infiltrated by hackers following the SolarWinds supply chain attack after they installed backdoored versions of the Orion IT monitoring platform. 80% of the identified victims are located in the United States and the rest of 20% is spread over seven other countries including Canada, Mexico, Belgium, Spain, the United Kingdom, Israel, and the UAE. What's certain is that, following the ongoing investigation of these attacks, "the number and location of victims will keep growing."

Read More on TheHackerNews

Microsoft identifies 40+ victims of SolarWinds hack, 80% from US

This is the last Kindred Security Newsletter for 2020

It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks during Christmas and New Year's Eve. But don't worry, we'll be back. See you soon for some awesome infosec news!

More #News

- Malicious Domain in SolarWinds Hack Turned into 'Killswitch'
- CORIE framework launched to test cyber resilience of Australia's financial services industry
- EU Unveils Revamp of Cybersecurity Rules Days After Hack
- Three million users installed 28 malicious Chrome or Edge extensions

- Microsoft Authenticator brings password autofill to mobile devices
- EU, Britain to Toughen Rules, Fines for Tech Giants
- New Windows malware may soon target Linux, macOS devices
- Top 10 Cybercrime and Cybersecurity Trends for 2021
- Exfiltrating Data from Air-Gapped Computers via Wi-Fi Signals (Without Wi-Fi Hardware)
- Cybersecurity: A Bleak 'Progress' Report
- How scammers target PayPal users and how you can stay safe
- SoReL-20M: A Huge Dataset of 20 Million Malware Samples Released Online
- Bouncy Castle crypto authentication bypass vulnerability revealed
- Operation SignSight: Supply–chain attack against a certification authority in Southeast Asia
- A breakthrough year for passwordless technology
- Becoming resilient by understanding cybersecurity risks: Part 2
- FBI Warns of DoppelPaymer Ransomware Attack Surge

#SolarWind

- Malicious Domain in SolarWinds Hack Turned into ‘Killswitch’
- New Evidence Suggests SolarWinds' Codebase Was Hacked to Inject Backdoor
- SolarWinds: The Hunt to Figure Out Who Was Breached
- SolarWinds Incident Response: 4 Essential Security Alerts
- Microsoft Says Its Systems Were Also Breached in Massive SolarWinds Hack
- SolarWinds hackers breach US nuclear weapons agency
- More on the SolarWinds Breach
- How to protect your organization following the SolarWinds compromise
- SolarWinds Supply Chain Hit: Victims Include Cisco, Intel

#Patch Time!

- SolarWinds Issues Second Hotfix for Orion Platform Supply Chain Attack
- Apple Patches Tens of Code Execution Vulnerabilities in macOS
- POS Device Makers Push Patches for Vulnerabilities
- WordPress plugin with 5 million installs has a critical vulnerability

#Tech and #Tools

- Risk8s Business: Risk Analysis of Kubernetes Clusters
- cloudquery: transforms your cloud infrastructure into queryable SQL tables for monitoring, governance and security.
- OWASP pytm - a Pythonic framework for Threat Modelling
- Automating Blind Sql Injection
- OAuth 2.0 authentication vulnerabilities
- The SolarWinds Orion SUNBURST supply-chain Attack
- How the SolarWinds Hackers Bypassed Duo’s Multi-Factor Authentication
- Connecting GoPhish with Office365
- Semgrep for Cloud Security

- Semgrep for Cloud Security
- Velociraptor and OSQuery
- solarflare: Credential Dumping Tool for SolarWinds Orion

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us