VERT Alert: SolarWinds Supply Chain Attack | Tripwire

By Tyler Reguly

Published: 2020-12-18 · Archived: 2026-04-06 02:53:05 UTC

Vulnerability Description

The United States Cybersecurity & Infrastructure Security Agency (CISA) has advised that an advanced persistent threat (APT) actor was able to insert sophisticated malware into officially signed and released updates to the SolarWinds network management software. The attacks have been ongoing since at least March 2020 and CISA has warned that many high-value targets within government, critical infrastructure, and the private sector have been compromised. Private security firm FireEye has also disclosed that the attackers were able to steal their private collection of hacking tools and techniques used for security audits.

Exposure and Impact

Successful compromise through the SolarWinds Orion backdoor could lead to complete compromise of a targeted network. Compromised network management software (NMS) provides deep access for an attacker to move laterally through a network and obtain credentials. Although not all organizations installing the backdoored version of the SolarWinds Orion software were necessarily compromised, all such organizations must assume that their network may be fully compromised.

Tripwire VERT recommends that all organizations review their systems for indicators of compromise related to the malicious SolarWinds updates as well as the FireEye Red Team Tools. Detected compromises should be handled through a security incident response process.

Tripwire IP360 users should have received ASPL updates.
To manually download this ASPL and/or its release notes: visit the Product Downloads section of the Tripwire Customer Center, select CONTENT > choose either the "VERT Ontology" link under NAME or the desired ASPL number link under TW UPDATE.

For Tripwire Enterprise users, we have released Tripwire Enterprise policy with tests for SUNBURST IoCs including file hashes for various versions of the compromised SolarWinds.Orion.Core.BusinessLayer.dll files and code signing certificates. Additionally, the policy contains file hash tests for FireEye's red team tools that were accessed by attackers.

To manually download this Tripwire Enterprise content, visit the Product Downloads section of the Tripwire Customer Center.

Detection

ASPL-920 includes the following Windows DRT checks related to the SolarWinds backdoor and associated exploitation:

- **SolarWinds netsetupsvc.dll Library Installed (ID: 467518)**
- **SolarWinds SolarWinds.Orion.Core.BusinessLayer.dll Library Backdoor (ID: 467516)**

ASPL-920 also includes the following checks for all vulnerabilities exploited by the FireEye hacking tools:

- **CVE-2019-11510**
  - Title: SA44101 - 2019-04: Pulse Connect Secure CVE-2019-11510 Arbitrary File Reading Vulnerability
  - ID: 432095 (non-DRT)
- **CVE-2020-1472**
  - Title: MS-2020-Aug: Netlogon Elevation of Privilege Vulnerability
  - ID: 451635 (Windows DRT)
  - SSH-DRT IDs: 459913, 459873, 459499, 459474, 459423, 459367, 459366, 459365, 459318, 459212, 459211, 459179
- **CVE-2018-13379**
  - Title: FortiOS CVE-2018-13379 Path Traversal Vulnerability
  - ID: 466495 (SSH-DRT & Non-DRT)
- **CVE-2018-15961**
  - Title: APSB18-33: Adobe ColdFusion Unrestricted File Upload Arbitrary Code Execution Vulnerability
  - ID: 447353 (Windows DRT), 447352 (SSH-DRT), 447310 (WebApp)
- **CVE-2019-0604**
  - Title: MS-2019-Feb: Microsoft SharePoint Remote Code Execution Vulnerability I
  - ID: 416822 (Windows DRT)
- **CVE-2019-0708**
  - Title: MS-2019-May: Remote Desktop Services Remote Code Execution Vulnerability
  - ID: 422448 (Windows DRT & Non-DRT)
- **CVE-2019-11580**
  - Title: Atlassian Crowd CVE-2019-11580 pdkinstall Vulnerability
  - ID: 35222 (Non-DRT & WebApp)
- **CVE-2019-19781**
  - Title: Citrix ADC Application Arbitrary Code Execution CVE-2019-19781 Vulnerability
  - ID: 437315 (Non-DRT)
- **CVE-2020-10189**
  - Title: Zoho ManageEngine CVE-2020-10189 Cewolfservlet RCE Vulnerability
  - ID: 467510 (Non-DRT)
- **CVE-2020-10189**
  - Title: Zoho ManageEngine CVE-2020-10189 Cewolfservlet Deserialization Vulnerability
  - ID: 467515 (Non-DRT)
- **CVE-2014-1812**

    - Title: MS14-025: Group Policy Preferences Elevation of Privilege Vulnerability
    - ID: 94146 (Windows DRT)
- **CVE-2019-3398**
    - Title: Atlassian Confluence Security Advisory 2019-04-17: Downloadallattachments Resource Path Traversal Vulnerability
    - ID: 422182 (WebApp)
- **CVE-2020-0688**
    - Title: MS-2020-Feb: Microsoft Exchange Memory Corruption Vulnerability
    - ID: 440153 (Windows DRT & Non-DRT)
- **CVE-2016-0167**
    - Title: MS16-039: Win32k Elevation of Privilege Vulnerability
    - ID: 226259 (Windows DRT)
- **CVE-2017-11774**
    - Title: MS-2017-Oct: Microsoft Outlook Security Feature Bypass Vulnerability
    - ID: 313178 (Windows DRT)
- **CVE-2018-8581**
    - Title: MS-2018-Nov: Microsoft Exchange Server Elevation of Privilege Vulnerability
    - ID: 412491 (Windows DRT)
- **CVE-2019-8394**
    - Title: Zoho ManageEngine Service Desk Plus CVE-2019-8394 File Upload Vulnerability
    - ID: 467517 (Windows DRT & Non-DRT)
