Cisco Security Advisory: SolarWinds Orion Platform Supply Chain Attack

Published: 2020-12-18 · Archived: 2026-04-05 22:50:27 UTC

- Due to the recent announcement by SolarWinds regarding compromises in their supply chain, SolarWinds has released a security advisory providing guidance on assessing and remediating this issue: https://www.solarwinds.com/securityadvisory

  Cisco recommends that customers assess if they have used an affected version of SolarWinds Orion Platform and, if so, take the following actions:

  1. Follow the guidance provided by the U.S. Department of Homeland Security and in the SolarWinds Security Advisory.
  2. Determine the need to change credentials on all devices being managed by the affected SolarWinds platform software. This includes:
     - User credentials
     - Simple Network Management Protocol (SNMP) version 2c community strings
     - SNMP version 3 user credentials
     - Internet Key Exchange (IKE) preshared keys
     - Shared secrets for TACACS, TACACS+, and RADIUS
     - Secrets for Border Gateway Protocol (BGP), OSPF, Exterior Gateway Routing Protocol (EIGRP), or other routing protocols
     - Exportable RSA keys and certificates for Secure Shell (SSH) or other protocols

  While there are no vulnerabilities in Cisco products related to this issue, if a customer was using an affected version of SolarWinds Orion Platform and would like to investigate potential impact to Cisco devices, Cisco has published a number of documents that can help the investigation. Please consult https://sec.cloudapps.cisco.com/security/center/resources/ir_escalation_guidance.

  For information on Cisco's use of SolarWinds in our enterprise environment, consult our Event Response Page here: https://sec.cloudapps.cisco.com/security/center/resources/solarwinds_orion_event_response

  Cisco TALOS has also published guidance regarding this issue that can be viewed here: https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

  Customers that need assistance with Incident Response activities can contact Cisco TALOS here: https://talosintelligence.com/incident_response

  Cisco will update this advisory as needed, if additional information becomes available.