# SolarWinds Orionプラットフォームサプライチェーン攻撃


アドバイザリーID : cisco-sa-solarwinds-supply-chain-attack
初公開日 : 2020-12-14 22:00
最終更新日 : 2020-12-18 14:16
バージョン 1.3 : Interim
回避策 : No workarounds available
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

SolarWindsが最近、サプライチェーンの侵害に関して発表したため、SolarWindsはこの問題の評価と修正に関するガイダンスを提供するセキュリティアドバイザリを公開しました。
https://www.solarwinds.com/securityadvisory

シスコでは、影響を受けるバージョンのSolarWinds Orionプラットフォームを使用しているかどうかを評価し、使用している場合は次の措置を講じることを推奨しています。

1. 米国国土安全保障省およびSolarWindsセキュリティアドバイザリに記載されているガイダンスに従ってください。
2. 影響を受けるSolarWindsプラットフォームソフトウェアによって管理されているすべてのデバイスのクレデンシャルを変更する必要があるかどうかを判断します。これには、次のような特徴があります。
    - ユーザクレデンシャル
    - Simple Network Management Protocol(SNMP)バージョン2cコミュニティストリング
    - SNMPバージョン3ユーザクレデンシャル
    - インターネットキー交換(IKE)事前共有キー
    - TACACS、TACACS+、およびRADIUSの共有秘密
    - ボーダーゲートウェイプロトコル(BGP)、OSPF、エクステリアゲートウェイルーティングプロトコル(EIGRP)、またはその他のルーティングプロトコルの秘密
    - セキュアシェル(SSH)またはその他のプロトコル用のエクスポート可能なRSAキーおよび証明書

この問題に関連するシスコ製品の脆弱性はありませんが、影響を受けるバージョンのSolarWinds Orionプラットフォームを使用しているお客様が、シスコデバイスに対する潜在的な影響を調査す

る必要がある場合、シスコは調査に役立つ多数のドキュメントを公開しています。https://sec.cloudapps.cisco.com/security/center/resources/ir_escalation_guidanceを参照してください。

シスコのエンタープライズ環境でのSolarWindsの使用については、https://sec.cloudapps.cisco.com/security/center/resources/solarwinds_orion_event_responseのEvent Response Pageを参照してください。

Cisco TALOSは、この問題に関するガイダンスも公開しています。このガイダンスについては、https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.htmlを参照してください。

インシデント対応アクティビティに関するサポートが必要なお客様は、Cisco TALOSに連絡してください。https://talosintelligence.com/incident_response

追加情報が入手可能になり次第、シスコはこのアドバイザリを随時更新します。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-solarwinds-supply-chain-attack

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.3 | 「Event Response Page」リンクを追加。 | 要約 | Interim | 2020-DEC-18 |
| 1.2 | 追加のソースを含むようにテキストを更新。 | 要約 | Interim | 2020-DEC-14 |
| 1.1 | ターロスリンクを更新。 | 要約 | Interim | 2020-DEC-14 |
| 1.0 | 初回公開リリース | — | Interim | 2020-DEC-14 |

## 利用規約

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。