

Cisco Secure Network Analytics ネットワークダイアグラムのアプリケーションクロスサイトスクリプティングの脆弱性

Medium アドバイザリーID : cisco-sa-sna-xss-mCA9tQnJ [CVE-2022-20741](#)
m 初公開日 : 2022-04-06 16:00 [20741](#)
バージョン 1.0 : Final
CVSSスコア : [5.4](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvz62478](#)

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

Cisco Secure Network Analytics (旧称Stealthwatch Enterprise) 用ネットワークダイアグラムアプリケーションのWebベース管理インターフェイスの脆弱性により、認証されたリモート攻撃者がインターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃を行う可能性があります。

この脆弱性は、該当ソフトウェアのWebベース管理インターフェイスによるユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたリンクをクリックするようにユーザを誘導することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスしたりする可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-mCA9tQnJ>

Attention (注意) : シスコポートフォリオの簡素化には、Cisco Secure という 1 つのブランドによるセキュリティ製品の名称変更が含まれます。詳細については、「[Cisco Secure が登場](#)」を参照してください。

該当製品

脆弱性のある製品

公開時点では、この脆弱性はCisco Secure Network Analyticsのネットワークダイアグラムアプリケーションに影響を与えました。

このアドバイザリの「修正済みソフトウェア」セクションを参照して、この公開時点で脆弱性が存在していたシスコソフトウェア [リリースに関する情報](#)を確認してください。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの [脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。](#)

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

[ソフトウェアのアップグレード](#)を検討する際には、[シスコ セキュリティ アドバイザリ ページ](#)で入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレードソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

修正済みリリース

発行時点では、次の表のリリース情報が正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグIDの「詳細」セクションを参照してください。

左側の列にはシスコソフトウェアリリースが一覧表示され、右側の列には、このアドバイザリに記載されている脆弱性の影響を受けたリリースと、この脆弱性に対する修正が含まれているリリースが表示されます。

のアプリケーションリリース	最初のリリース)
2.1.1 より前	2.1.1

Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group (ASIG) による内部セキュリティテストで発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-mCA9tQnJ>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	最終版	2022年4月6日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

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、単独の転載や意識を施した場合、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。