

Cisco Security ManagerのJavaデシリアライゼーションの脆弱性



アドバイザリーID : cisco-sa-20191002-sm- [CVE-2019-](#)

java-deserial

[12630](#)

初公開日 : 2019-10-02 16:00

バージョン 1.0 : Final

CVSSスコア : [6.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvj29055](#)

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 Security Managerで使用されるJavaデシリアライゼーション機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスで任意のコマンドを実行する可能性があります。

この脆弱性の原因は、該当ソフトウェアでユーザが入力したコンテンツが安全に逆シリアル化されないことにあります。シリアル化された悪意のある Java オブジェクトが該当デバイスの特定のリスナーに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者はcasuserの権限を使用してデバイスで任意のコマンドを実行でき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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-sm-java-deserial>

該当製品

脆弱性のある製品

公開時点では、この脆弱性はリリース4.18より前のCisco Security Managerリリースに影響を与えました。

最も完全で最新の情報については、このアドバイザリーの上部にあるバグ 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

Java Management Extension Remote Method Invocation(JMX RMI)は、デフォルトでポート 1099を使用します。この脆弱性を軽減するには、JMX RMIサービスを無効にします。推奨される方法は、Cisco Security Managerをリリース4.18以降にアップグレードすることです。これが不可能な場合は、Cisco Technical Assistance Center(TAC)に連絡して、レジストリを編集してJMX RMIポートを無効にするスクリプトを入手してください。

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、[シスコのセキュリティアドバイザリおよびアラート (Cisco Security Advisories and Alerts)] 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完全なアップグレードソリューション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、TACまたは契約した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

公開時点では、Cisco Security Managerリリース4.18以降にこの脆弱性に対する修正が含まれています。

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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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を確認していません。

出典

シスコは、この脆弱性を報告していただいたGoogleのFrancisco Ribeiro氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa->

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	—	Final	2019年10月2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。

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。