Cisco Secure Access Control System の Java 逆シリアル化における脆弱性

Critical

アドバイザリーID : cisco-sa-20180307-acs2

初公開日 : 2018-03-07 16:00

バージョン 1.0 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCvh25988

CVE-2018-0147

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 Access Control System（ACS）で使用されている Java 逆シリアル化における脆弱性により、未認証のリモート攻撃者に、該当デバイス上で任意のコマンドを実行され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。 攻撃者は、シリアライズされた Java オブジェクトを巧妙に細工して送信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。 不正利用に成功すると、*root* 権限を使用してデバイス上で任意のコマンドを実行する恐れがあります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs2

該当製品

脆弱性のある製品

この脆弱性は、リリース 5.8 パッチ 9 より前のすべての Cisco Secure ACS リリースに影響します。デバイスで実行されている Cisco Secure ACS のリリースを確認するには、管理者権限で、次のいずれかの方法を実施します。

Cisco Secure ACS コマンドライン インターフェイス

Cisco Secure ACS CLI から **show version** コマンドを実行できます。 たとえば、Cumulative Patch 1 がインストールされた Cisco Secure ACS 5.8.0.32 を実行するデバイスの場合、 **show version** コマンドの出力は、次の例のようになります。

```
acs5x/admin# show version

Cisco Application Deployment Engine OS Release: 2.2
ADE-OS Build Version: 2.2.2.013
ADE-OS System Architecture: x86_64

Copyright (c) 2005-2015 by Cisco Systems, Inc.
All rights reserved.
Hostname: acs5x


Version information of installed applications
---------------------------------------------


Cisco ACS VERSION INFORMATION
-----------------------------
Version : 5.8.0.32
Internal Build ID : B.442
Patches :
5-8-0-32-1

acs5x/admin#
```

Cisco Secure ACS Web ベース インターフェイス

Cisco Secure ACS Web ベース インターフェイスにログインし、画面右上隅の [バージョン情報 (About)] リンクをクリックします。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

この脆弱性に割り当てられている CVSSv3 スコアは、5.8 パッチ 7 より前の Cisco Secure ACS リリースに基づいています。 リリース 5.8 パッチ 7 またはパッチ 8 を実行している Cisco Secure ACS システムの場合、この脆弱性を不正利用するためには認証が必要になります。 リリース 5.8 パッチ 7 またはパッチ 8 を実行する Cisco Secure ACS システムに割り当てられた CVSSv3 スコアは、 Base 8.8: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H です。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、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、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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は、Cisco Secure ACS 5.8.0.32.9 Cumulative Patch で修正されています。 このソフトウェアは Cisco.com の Software Center でダウンロードできます（[製品（Products）] > [セキュリティ（Security）] > [ネットワークの可視性と適用（Network Visibility and Enforcement）] > [Secure Access Control System] > [Secure Access Control System 5.8]）。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されてい

る脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性を発見して報告いただいた Positive Technologies 社のセキュリティ研究者、Mikhail Klyuchnikov 氏と Yury Aleynov 氏に謝意を表します。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs2

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 3 月 7 日

利用規約