

Cisco HyperFlex ソフトウェアのコマンド インジェクションにおける脆弱性



アドバイザーID : [cisco-sa-20190220-hyperflex-injection](#) [CVE-2018-15380](#)
初公開日 : 2019-02-20 16:00
最終更新日 : 2019-10-23 18:41
バージョン 2.0 : Final
CVSSスコア : [8.8](#)
回避策 : Yes
Cisco バグ ID : [CSCvq24176](#) [CSCvj95606](#)

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 HyperFlex ソフトウェアのクラスタ サービス マネージャの脆弱性により、認証されていない隣接攻撃者が root ユーザとしてコマンドを実行する可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、クラスタ サービス マネージャに接続し、バインドされたプロセスにコマンド インジェクションを行うことにより、この脆弱性をエクスプロイトします。エクスプロイトに成功すると、攻撃者は、影響を受けるホストで root ユーザとして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。本脆弱性に対処する回避策がいくつかあります。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyperflex-injection>

該当製品

脆弱性のある製品

この脆弱性は、3.5(2g) より前の Cisco HyperFlex ソフトウェアリリースに影響を及ぼします。

HyperFlex ソフトウェア リリースの確認

インストールされている Cisco HyperFlex ソフトウェアのリリースを確認するために、管理者

は CLI または GUI を使用できます。

CLI を使用する場合、管理者は `stcli about` コマンドを発行できます。デバイスが Cisco HyperFlex ソフトウェア リリース 3.0(1d) を実行している場合、コマンドの出力例は次のようになります。

```
<#root>
```

```
root@hxccluster:~#
```

```
stcli about
```

```
serviceType: stMgr
instanceUid: c4f0441c-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
name: HyperFlex StorageController
locale: English (United States)
serialNumber: WZP#####OCD,WZP#####OG9,WZP#####
apiVersion: 0.1
modelName: HX240C-M5L
build: 3.0.1d-29754 (internal)
displayVersion:
```

```
3.0(1d)
```

```
fullName: HyperFlex StorageController 3.0.1d
productVersion: 3.0.1d-29754
```

GUI を使用する場合、管理者は HX Connect にログイン後、ページの左下にある [バージョン情報 (About)] リンクをクリックできます。

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

この脆弱性の回避策は、修整版リリースにアップグレードできないお客様に使用できます。回避策の実装の調整に関しては、 [Cisco Technical Assistance Center \(TAC\)](#) にお問い合わせください。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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です。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、[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、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 Cisco Service Contract 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 POS 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 HyperFlex 3.5(2g) で修正されています。

ソフトウェアアップデートは、Cisco.com の [Software Center](#) から次の手順でダウンロードできます。

1. [すべてを参照 (Browse All)] をクリックします。
2. [ハイパーコンバージド インフラストラクチャ (Hyperconverged Infrastructure)] > [HyperFlex HX データ プラットフォーム (HyperFlex HX Data Platform)] を選択します。
3. [HyperFlex HX データ プラットフォーム (HyperFlex HX Data Platform)] ページの左側のペインを使用して各リリースにアクセスします。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyperflex-injection>

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.0	修正済みリリースを更新。障害に関する記述を追加。	「脆弱性のある製品」および「修正済みソフトウェア」	Final	2019年10月23日
1.1	回避策を更新。	回避策	Final	2019年4月4日
1.0	初回公開リリース	—	Final	2019年2月20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。